2011 American Control Conference
on O'Farrell Street, San Francisco, CA, USA
June 29 - July 01, 2011

Inequality-Based Reliability Estimates for Complex Systems

Stacy D. Hill, James C. Spall, and Coire J. Maranzano

Abstract—Full-system testing for large-scale systems is often infeasible or very costly. Thus, when estimating system reliability, it is desirable to employ a method that uses subsystem tests, which are often less expensive and more feasible. This paper presents a method for bounding full-system reliabilities based on subsystem tests and, if available, full system tests. The method does not require that subsystems be independent. It accounts for dependencies through use of certain probability inequalities. The inequalities provide the basis for valid reliability calculations while not requiring independent subsystems or full-system tests. The inequalities allow for test information on pairwise subsystem failure modes to be incorporated, thereby improving the estimate of system reliability. We illustrate some of the properties of the estimate via an example application.

I. Introduction

It is often infeasible or very costly to assess the performance of complex systems[1] through full-system tests. Further, full-system testing may sometimes involve the destruction of expensive system assets or is limited by operational policy. There is a critical need for alternate approaches to estimating full system reliability or other performance characteristics, especially for systems that require non-destructive tests such as bridges, machines, aircraft, satellites, and weapon systems. In addition to the need to minimize the number of full system tests, it is desirable to exploit valuable information from subsystem tests (which tend to be performed as part of the development of complex systems and are less expensive than full system tests) as a means of quantifying full system reliability. Of the various system performance characteristics, system reliability—the focus of this paper—is one that is usually difficult to quantify without the benefit of full system testing.

Many approaches exist for quantifying system reliability from subsystem tests (see, e.g., [1], [2], [3], [4]). These methods, however, assume that the subsystems are statistically independent or that the system configuration is completely specified. Assuming subsystem independence or a particular subsystem configuration is often erroneous for complex systems, which may contain many interdependent subsystems that interact in subtle and not-so subtle ways (for the method in [4], however, this problem is overcome by developing a test program consisting of a mixture of full system and subsystem tests that is robust to system configuration mis-modeling [5]). Under the assumption of independence for a series system, reliability is calculated as the product of all the critical subsystem reliabilities. For such systems, reliability calculations that rely on independence can be misleading.

To illustrate the effect of violating the independence assumption on the system reliability calculation consider the following simple example. Suppose the system consists of component subsystems S_i, i = 1, 2, 3, …, 20, which fail if some parameter X_i exceeds a specified threshold, $X_i > 2.5$ say. Assume that the X_i's are zero mean, normal random variables with $\mathrm{var}(X_i) = 1$ for all i and $\mathrm{cov}(X_i, X_j) = 0.75$ when $i \neq j$. The probability of system failure is $p = 1 - P\left(\bigcap_i \{X_i \le 2.5\}\right) = 0.042$. If it were assumed, erroneously, that the X_i's were independent, then we would obtain $p = 1 - \prod_i P\{X_i \le 2.5\} = 0.117$. Hence, in assuming independence, one would produce a probability of system failure that is greater than twice the true failure probability. If a significant number of the subsystem-to-subsystem covariances were negative (rather than positive as in this example), then a reliability calculation based on the assumption of independence would underestimate the probability of failure. Obviously, such errors can have potentially serious consequences in system design or analysis.

We present a new method of quantifying system reliability that overcomes some of the major shortcoming of previous approaches. The method, called *Inequality-Based Reliability* (IBR), makes use of results from subsystem tests and (if available) full-system tests. IBR combines estimates of two quantities to bound system reliability: an estimate of an upper bound on the system failure probability (derived from the subsystem tests) and a point estimate of system reliability (computed from system-level tests). The IBR estimate is a combination of these two estimates defined to minimize a certain mean-square error.

The upper bound estimate—which provides an initial upper bound estimate on the system failure probability—makes use of information about the probability of failure for the individual subsystems and the joint probability of failure for specified pairs of subsystems. Pairwise failure probabilities are not required in order to employ the IBR method, but use of the pairwise information improves the upper bound estimate. The combination of the upper bound estimate with a full system probability of failure estimate is what distinguishes IBR from other methods of system reliability assessment.

II. Probability Inequalities

We present probability inequalities and results useful in defining the IBR estimate (Section 3). Suppose that a system consists of $m > 1$ critical subsystems that have two states—operating or failure. The system fails if one or more of its subsystems fails. In other words, the sub-systems can be viewed as being serially connected. Let F_i denote the event that subsystem i fails, p_i its probability of failure, and $F = \bigcup F_i$ the event of system failure. The probability p of system failure is $p = P\left(\bigcup F_i\right) = 1 - P\left(\bigcap F_i^c\right)$.

The authors are with the Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland 20723-6099 U.S.A. (stacy.hill@jhuapl.edu, james.spall@jhuapl.edu, coire.maranzano@jhuapl.edu). This work was supported in part by the JHU/APL IRAD Program and U.S. Navy Contract N00024-03-D-6606.

[1] Complex systems are often thought of as systems of systems. To avoid the need to repeatedly refer to tests on systems, subsystems, components, processes, and other aspects of the full system as the key source of information other than full system tests, we will usually only refer to subsystem tests; subsystem tests in this context should be considered a proxy for all possible test information short of full system tests.

In general, $p \neq 1-\prod_{i=1}^{m}(1-p_i)$, since the F_i's are not assumed to be independent. The exact expression for p contains sums and differences involving up to $2^m - 1$ joint probabilities $P_J = P\left(\bigcap_{i \in J} F_i\right)$, where the index set J varies over all the non-empty subsets of $1,2,\ldots,m$. For complex systems, obtaining estimates of all the joint probabilities will usually be infeasible. The IBR reliability estimate relies on upper bounds on p and requires, for its computation, at most *pairwise* failure probabilities; hence, it only involves the p_i's and $p_{ij} = P\left(F_i \bigcap F_j\right),\ 1 \le i, j \le m$.

Upper bounds, for the probability of a union of sets, which depend on at most pairwise intersections, were derived in [6], [7], and [8] using graph-theoretic results. We briefly summarize the relevant results.

Consider the set $T \equiv \left\{\{i,j\} : i \neq j, 1 \le i, j \le m\right\}$ consisting of all possible *edges* between the *vertices* $\{1,2,\ldots,m\}$. A subset of T is a *graph*.

Proposition 1. ([6], [7]) Suppose τ is a graph, then

$$p \le \sum_i p_i - \sum_{\{i,j\} \in \tau} p_{i,j} \tag{1}$$

if and only if τ satisfies the following two conditions:
(i) for each $i = 1,\ldots,m' \le m$, there is a $j \neq i$, $1 \le j \le m'$, such that the edge $\{i,j\}$ belongs to τ (i.e., each vertex is connected to at least one other vertex different from itself);
(ii) τ contains exactly $m' - 1$ edges (i.e., τ has no cycles).

Proposition 1 states that inequality (1) holds for *spanning trees* in T, which are graphs satisfying condition (i) and condition (ii) for $m' = m$. By definition a spanning tree is a graph that consists of exactly $m - 1$ branches such that at least one edge is incident on each vertex. The proposition states that inequality (1) also holds more generally for all *trees* in T, which, by definition are spanning trees on a subset of the vertices $\{1,2,\ldots,m\}$.

Denote the upper bound on the right side of (1) corresponding to a particular choice of τ by $p_{UB}(\tau)$. (The τ will sometimes be suppressed for convenience, when there is no chance of confusion.) From (1) we have the following upper bound for p ([6], [7]):

$$p \le \min_{\tau} p_{UB}(\tau), \tag{2}$$

where the minimum are taken over all trees in T. Note that if τ is a spanning tree and τ' is a tree contained in τ then $p_{UB}(\tau) \le p_{UB}(\tau')$. Thus, spanning trees provide the best possible upper bounds over all trees.

Figure 1. illustrates all possible upper bounds computed from (1) for a system consisting of three subsystems. The set T consists of the edges $\{1,2\}$, $\{1,3\}$ and $\{2,3\}$, which denote all possible pairs of subsystems. The example pairwise probabilities are given in the figure. Also, the system failure probability p is computed assuming that the simultaneous failure probability of all three systems equals 0.01. Each upper bound is greater than or equal to the true system failure probability (which equals 0.10) and is less than or equal to the well-known Bonferroni bound $\sum_i p_i$ = 0.18. Note that the minimum bound derived from (2) is 0.11 and is obtained by taking the minimum of $p_{UB}(\tau)$ over all trees τ in T. Note that any joint failure probability has the potential to improve upon the Bonferroni bound as illustrated by examining the bounds associated with the trees in T.

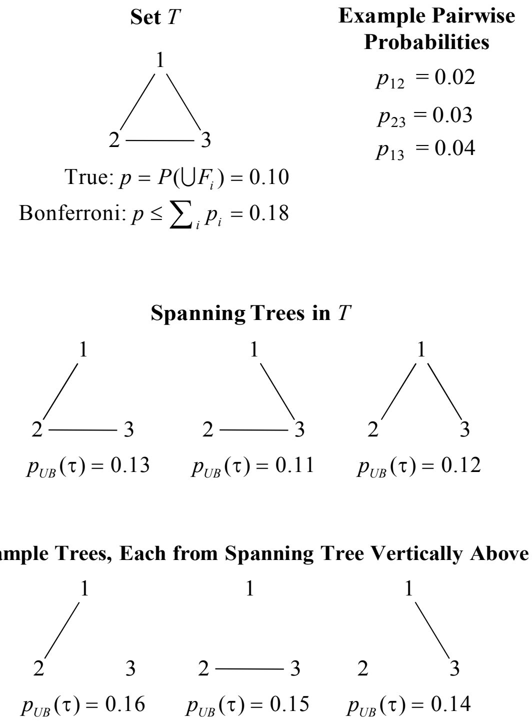

Figure 1. Example upper bound probabilities in (1) corresponding to the spanning trees and trees for a system consisting of three subsystems.

In most applications, estimates of the probability $P\left(F_i \bigcap F_j\right)$ will only be available for *some* pairs of events. It is of interest, then, to consider upper bounds in (1), or bounds derived from them, that use only a subset of the pairwise probabilities. In particular, consider the following upper bounds derived from (1):

$$p \le \sum_i p_i - (2/m)\sum_{i<j} p_{ij} \quad ([9]) \tag{3}$$

$$p \le \sum_i p_i - \sum_i p_{i,i+1} \quad ([7]) \tag{4}$$

$$p \le \sum_i p_i - \max_j \sum_{i \neq j} p_{ij} \quad ([10]) \tag{5}$$

$$p \le \sum_i p_i - \sum_{i=2}^{m} \max_{k<i} p_{ik} \quad ([11]). \tag{6}$$

All the inequalities (1) – (6) improve on the Bonferroni inequality. The upper bound (4), as will be shown, corresponds to a particular spanning tree, whereas the other bounds are derived from spanning tree inequalities.

It is easy to see that (4) holds. Indeed, the index set consisting of $\{i, i+1\}$, $i = 1,\ldots, m-1$, is a spanning tree. Hence,

$$\sum_i p_i - \max_{\tau}\left\{\sum_{(i,j)\in\tau} p_{ij}\right\} \le \sum_i p_i - \sum_i p_{i,i+1},$$

from which (4) follows. We show next that the other bounds—(3), (5), and (6)—are greater than or equal to the least upper bound in (2). In particular, we have the following result:

Proposition 2. Let $p^* = \min_{\tau}\left\{\sum_i p_i - \sum_{(i,j)\in\tau} p_{ij}\right\}$. Then, bounds (3), (5), and (6) satisfy:

(i) $p^* \le \sum_i p_i - \max_j \sum_{i\ne j} p_{ij} \le \sum_i p_i - (2/m)\sum_{i<j} p_{ij}$

(ii) $p^* \le \sum_i p_i - \sum_{i=2}^{m} \max_{k<i} p_{ik}$

Proof. To prove (i), note that the graph $\{\{i,j\} : i = 1,\dots,m, i \ne j\}$ is a spanning tree for each j; hence $p^* \le \sum_i p_i - \sum_{i\ne j} p_{ij}$. This inequality implies

$$p^* \le \sum_i p_i - \max_j \sum_{i\ne j} p_{ij} \le \sum_i p_i - \sum_{i\ne j} p_{ij},$$

which, when averaged over $j = 1, \dots, m,$ yields

$$p^* \le \sum_i p_i - \max_j \sum_{i\ne j} p_{ij} \le \sum_i p_i - \frac{1}{m}\sum_j \sum_{i\ne j} p_{ij}.$$

The preceding inequality and the identity $\sum_j \sum_{i\ne j} p_{ij} = 2\sum_{i<j} p_{ij}$ complete the proof of (i).

Last, to prove (ii), note that the index set consisting of $\{i, k_i\}$, $i = 2,\dots,m$, is a spanning tree if for each i, $1 \le k_i < i$, $i = 2, 3, \dots, m$, in which instance $p^* \le \sum_i p_i - \sum_{i=2}^{m} p_{i,k_i}$. If, in addition k_i is chosen so that $p_{i,k_i} = \max\{p_{i,j} : 1 \le j < i\}$, $i = 2, 3, \dots, m$, then $\sum_i p_i - \sum_{i=2}^{m} p_{i,k_i} = \sum_i p_i - \sum_{i=2}^{m} \max_{i<k} p_{ik}$, from which the result follows. *Q.E.D.*

Given an estimate $\hat{p}_i$ of p_i and $\hat{p}_{ij}$ of p_{ij}, $1 \le i,j \le m$, we can form an upper bound estimate $\hat{p}_{UB}$ by substituting the estimates in the right-side of (2) (or (3) through (6) and taking the smallest of the four bounds). Also, note that inequalities (1) – (6) can be further adapted to use available estimates of the probability $P(F_i \cap F_j)$ by taking advantage of the fact that inequality (1) holds for all trees on the vertices $\{1,2,\dots,m\}$. (See Figure 1. for example.) Typically, $\hat{p}_i$ would be computed simply as the ratio $\{\text{\# failures}\}/\{\text{\# trials}\}$ for subsystem i. The estimation of the joint probabilities $\hat{p}_{ij}$ is typically more challenging and problem-dependent. Usually their derivation will involve physical modeling and system identification together with subsystem tests. In particular, failure detection and fault isolation methods ([12], [13], [14], [15]) may provide a means of estimating such joint probabilities. Further, fault isolation methods are valuable in providing a means for determining the specific cause of a failure.

Remark: Although the bound in (5) is sharper than (3), it is easier to derive uncertainties and confidence intervals for (3) than (5), since it does not involve finding a maximum. (See Section 3.C).

III. THE IBR METHOD

A. Computation of the Estimate

We now describe the IBR estimate. The approach recognizes the practical reality when one may have at least a few full system tests that contain valuable information to be combined with the subsystem tests. It is not necessary, however, to have full-system tests to implement the IBR approach. If full-system test results are available, the IBR estimate here is a weighted combination of the upper bound estimate $\hat{p}_{UB}$ and the estimate $\hat{p}$ based on full-system testing. (The estimate $\hat{p}$ is usually computed simply as the ratio of number of failures to the number of tests.) In the absence of full system testing—i.e., $\hat{p}$ is unavailable— $\hat{p}_{UB}$ is defined to be the IBR estimate.

Assume that $\hat{p}_{UB}$ and $\hat{p}$ are derived from independent data. For each λ, $0 \le \lambda \le 1$, let $p_\lambda(\tau) = \lambda p + (1-\lambda) p_{UB}(\tau)$. For each λ, the quantity $\hat{p}_\lambda(\tau) = \lambda\hat{p} + (1-\lambda)\hat{p}_{UB}(\tau)$ is an (upper bound) estimator of p. The IBR estimate of p (based on $\hat{p}$, $\hat{p}_{UB}$ and, hence, τ) is obtained by suitably choosing λ. In particular, the IBR estimate is defined to be $\hat{p}_{\lambda^*}(\tau) = \lambda^*\hat{p} + (1-\lambda^*)\hat{p}_{UB}(\tau)$, where λ^* is chosen so that $\hat{p}_{\lambda^*}(\tau)$ minimizes the mean square error $E\left[(\hat{p}_\lambda - p_\lambda)^2\right]$ over all λ such that $0 \le \lambda \le 1$. In particular, as will be shown (see Section 3.3), $\hat{p}_{\lambda^*}(\tau) = \lambda^*\hat{p} + (1-\lambda^*)\hat{p}_{UB}(\tau)$, where $\lambda^* = \sigma_{UB}^2/(\sigma^2 + \sigma_{UB}^2)$, $\sigma_{UB}^2 = E\left[(\hat{p}_{UB} - p_{UB})^2\right]$, and $\sigma^2 = E\left[(\hat{p} - p)^2\right]$. In practice, estimates of σ^2 and σ_{UB}^2 would be used to form an estimate of λ^*, say $\hat{\lambda}^*$.

B. Discussion of the Estimate

In this subsection, we provide justification of the loss function for defining the IBR estimate. According to the foregoing, the IBR estimate is the estimate of the form $\hat{p}_\lambda$ that minimizes the mean square error $E\left[(\hat{p}_\lambda - p_\lambda)^2\right]$. What typically is of interest in practice is the error $E\left[(\hat{p}_\lambda - p)^2\right]$, where p is the true system reliability. However, this latter quantity depends on the bias term $(p - p_{UB})^2$, which is unknown.

Proposition 3 below establishes a bound on the error in using $E\left[(\hat{p}_\lambda - p_\lambda)^2\right]$ rather than $E\left[(\hat{p}_\lambda - p)^2\right]$ to define the IBR estimate.

Proposition 3. Let $\hat{p}_{\lambda^{**}}$ minimize $E\left[(\hat{p}_\lambda - p)^2\right]$ and let $\hat{p}_{\lambda^*} = \lambda^*\hat{p} + (1-\lambda^*)\hat{p}_{UB}$ be the IBR estimate of p. Then

$$\left|E\left[(\hat{p}_{\lambda^{**}} - p)^2\right] - E\left[(\hat{p}_{\lambda^*} - p_{\lambda^*})^2\right]\right| \le (p - p_{UB})^2.$$

Proof. Observe that $p - \hat{p}_\lambda = p - p_\lambda + p_\lambda - \hat{p}_\lambda = (1-\lambda)(p - p_{UB}) + (p_\lambda - \hat{p}_\lambda)$, which implies

$$E\left[\left(\hat{p}_\lambda - p\right)^2\right] = (1-\lambda)^2 \left(p - p_{UB}\right)^2 + E\left[\left(\hat{p}_\lambda - p_\lambda\right)^2\right].$$

If λ^{**} minimizes $E\left[\left(\hat{p}_\lambda - p\right)^2\right]$, the last identity implies that

$$E\left[\left(p-\hat{p}_{\lambda^{**}}\right)^2\right] = \left(1-\lambda^{**}\right)^2 \left(p - p_{UB}\right)^2 + E\left[\left(\hat{p}_{\lambda^{**}} - p_{\lambda^{**}}\right)^2\right]$$

$$\geq \left(1-\lambda^{**}\right)^2 \left(p - p_{UB}\right)^2 + \min_\lambda E\left[\left(\hat{p}_\lambda - p_\lambda\right)^2\right].$$

Since $(1-\lambda)^2 \leq 1$, we also have

$$\left(p - p_{UB}\right)^2 + E\left(\hat{p}_{\lambda^*} - p_{\lambda^*}\right)^2 \geq E\left(p - \hat{p}_{\lambda^{**}}\right)^2.$$

Consequently,

$$\left|E\left[\left(\hat{p}_{\lambda^{**}} - p\right)^2\right] - E\left[\left(\hat{p}_{\lambda^*} - p_{\lambda^*}\right)^2\right]\right| \leq \left(1-\lambda^{**}\right)^2 \left(p - p_{UB}\right)^2$$

$$\leq \left(p - p_{UB}\right)^2.$$

Q.E.D.

Note that the right most term in the above is simply the square of the error in p_{UB}.

Next, we establish a connection between the IBR estimate $\hat{p}_{\lambda^*}(\tau)$ and the method of least squares by deriving the optimal value λ^* of λ. For the connection between IBR and least squares we prove the following result.

Proposition 4. Let $\hat{p}$ and $\hat{p}_{UB}$ be unbiased, independent estimates of *p* and p_{UB}, respectively. Then,

(i) $p \leq E\left(\min_\tau \hat{p}_{\lambda^*}(\tau)\right) \leq \min_\tau p_{\lambda^*}(\tau)$, where the τ values belong to a specified set of *J* of spanning trees.

(ii) If $\hat{p}_{\lambda^*}$ is the IBR estimate *p*, then $\lambda^* = \sigma_{UB}^2 / \left(\sigma^2 + \sigma_{UB}^2\right)$, where $\sigma_{UB}^2 = E\left[\left(\hat{p}_{UB} - p_{UB}\right)^2\right]$ and $\sigma^2 = E\left[\left(\hat{p} - p\right)^2\right]$.

Proof. The proof of (i) is omitted since it is straightforward. Now consider (ii). First,

$$\begin{aligned} E\left[\left(\hat{p}_\lambda - p_\lambda\right)^2\right] &= \lambda^2 E\left[\left(\hat{p} - p\right)^2\right] \\ &\quad + 2\lambda(1-\lambda)\, E\left[\left(\hat{p} - p\right)\left(\hat{p}_{UB} - p_{UB}\right)\right] \\ &\quad + (1-\lambda)^2\, E\left[\left(\hat{p}_{UB} - p_{UB}\right)^2\right] \\ &= \lambda^2 E\left[\left(\hat{p} - p\right)^2\right] + (1-\lambda)^2\, E\left[\left(\hat{p}_{UB} - p_{UB}\right)^2\right], \end{aligned} \tag{7}$$

where the last identity follows from the independence of $\hat{p}$ and $\hat{p}_{UB}$. Using the method of Lagrange multipliers, it can be shown that the right-side of (7) attains its minimum at $\lambda^* = \sigma_{UB}^2 / \left(\sigma^2 + \sigma_{UB}^2\right)$. *Q.E.D.*

In practice, increasing the number of subsystem tests relative to the number of full system tests drives λ^* to zero and reduces the variability of the IBR estimate (decreases the uncertainty in the estimate). However, increasing the number of subsystem tests used to estimate subsystem or joint subsystem probabilities of failure *cannot* move the IBR estimate closer to the true unknown system probability of failure *p*, because $\hat{p}_{UB}$ is a bound. Thus, increasing the number of subsystem tests relative to the number of full system tests moves the IBR estimate closer to a true unknown bound determined by the bounding method used to form $\hat{p}_{UB}$. This and other properties of the IBR estimate are demonstrated via simulation in [16].

C. *Confidence Intervals*

We also derive confidence intervals for the IBR estimate in terms of the uncertainties in $\hat{p}$ and $\hat{p}_{UB}$. Because there is no known finite-sample distribution for $\hat{p}_{\lambda^*}$, confidence intervals rely on the asymptotic distributions of the estimates $\hat{p}$, $\hat{p}_i$ and $\hat{p}_{jk}$. These confidence intervals are useful in expressing the uncertainty in $\hat{p}_{\lambda^*}$ as an estimate of $\hat{p}_{\lambda^*}$. (As noted previously, the estimate $\hat{p}$ of *p* is based on full system testing and is the total number of system failures in *n* trials.) Assume that the other two estimates are based on individual and pairwise subsystem testing. Thus, $\hat{p}_{jk}$ is the ratio of the number of failures to the total number of trials that occurred when operating subsystems *j* and *k* simultaneously. (As noted in the previous section, the estimate $\hat{p}_{jk}$ may be derived by other means. See, e.g., [12].) Let φ denote *p*, p_i, or p_{jk}, and let $\hat{\varphi}(n)$ denote the estimate of φ, where *n* is the number of trials. Then $\sqrt{n}\left(\hat{\varphi}(n) - \varphi\right) \xrightarrow{\text{dist}} N\left(0, \varphi(1-\varphi)\right)$ as $n \to \infty$. Again, fix τ and let p_{UB} denote the bound on the right-side of (1), and let $\hat{p}_{UB}$ denote its estimate. (As before, we suppress τ, since there is no chance of confusion.)

The estimator $\hat{p}_{UB}$ is asymptotically normal,

$$\sqrt{n}\left(\hat{p}_{UB} - p_{UB}\right) \xrightarrow{\text{dist}} N\left(0, \sigma^2\right),$$

where $\sigma^2 = \sum p_i(1-p_i) + \sum_{\{i,j\}\in\tau} p_{ij}(1-p_{ij})$. Two special cases of σ^2 for the inequalities in (3) and (4) are, respectively,

$$\sigma_B^2 = \sum p_i(1-p_i) + \frac{4}{m^2} \sum_{i<j} p_{ij}(1-p_{ij}) \quad \text{and}$$

$$\sigma_B^2 = \sum p_i(1-p_i) + \sum_{i<m} p_{i,i+1}(1-p_{i,i+1}).$$

Using the asymptotic normality of $\hat{p}_{UB}$ and $\hat{p}$, we can derive approximate confidence intervals about $\hat{p}_{\lambda^*}$ (similar to those obtained by [17]). The $100(1-\alpha)\%$ confidence interval, where $0 \leq \alpha \leq 1$, is given by:

$$\hat{p}_{\lambda^*} \pm z\sqrt{(\lambda^*)^2 p(1-p) + \left(1-\lambda^*\right)^2 \sigma^2},$$

where *z* is the upper $100\alpha/2$ percent point of the standard normal distribution. Of course, in practice, estimates of σ^2 would be used in the construction of the confidence limits.

D. *Fictitious Test for Use Without Observed System Failures*

There are difficulties in getting a meaningful estimate of the failure probability when there are no observed failures in the full system tests. This, in fact, will be a typical situation when the system has high reliability and the number of full system tests is small, both of which are expected for typical applications of IBR. Of course, this problem is not unique to IBR. Any non-Bayesian method will have problems in getting an estimate of a failure probability with an (unknown) true value that is non-zero when there are no observed failures! We show here how a fictitious $(n + 1)$st full system test can be incorporated into the IBR framework when there are no observed failures in the full system tests.

It is clear that $\hat{p} = \hat{\sigma}^2 = 0$ when there are no observed failures in the full system tests, where $\hat{\sigma}^2$ is the estimate of σ^2. Consequently, the IBR estimate is $\hat{p}_{\lambda^*} = 1\times 0 + 0\times \hat{p}_{UB} = 0$, which is not generally satisfactory. (Although this estimate is unsatisfactory in the application to a real-world system, it actually makes intuitive sense when considering that the variance estimate of 0 indicates "perfect" knowledge of p.) We may address this practical shortcoming by focusing on the need for an *upper bound* to p. Assume a fictitious $(n + 1)$st full system test that is a failure. This represents a "worst case" for the system, consistent with forming an upper bound to the failure probability. Now, we have $\hat{p} = 1/(n+1)$ and $\hat{\sigma}^2 = \hat{p}(1-\hat{p})/(n+1) = n/(n+1)^3 > 0$. This strictly positive variance estimate allows for a meaningful IBR estimate to be formed. Note also that this variance estimate is biased upwards by the fact that $\hat{p}$ is "too large." This bias causes a slight down-weighting of the full system test information when forming $\hat{p}_{\lambda^*}$, which is correct in the sense that the fictitious failure would not likely have occurred in a real $(n + 1)$st full system test.

IV. IBR FOR SERIES-PARALLEL SYSTEM WITH REPEATED COMPONENTS

It is possible to derive an expression for $\hat{p}_{UB} = \hat{p}_{UB}(\tau)$ for specific systems. Consider, for example, a series-parallel system with arbitrarily repeated components. In such systems, the same component-type may appear multiple times in different subsystems. Different components are assumed to function independently; however, reliability estimates for components of the same type are estimated from the same data. Thus, the subsystem reliability estimates are dependent.

A reliability estimate for systems that depend on pairwise subsystem failure probabilities was derived in [18]. The estimate in [18], however, provides a *lower bound* on the failure probability (see, e.g., [8]). It is desirable to have an *upper bound* on the probability of failure. The estimate in [18] can be modified to provide such a bound.

The upper bound estimates for series-parallel system are given as follows. Suppose there are a fixed number of component types and that each subsystem is composed of a finite number of components, some of which are repeated in parallel. Following [18], let q_h denote the failure probability of the hth component type, k_{ih} denote the number of components of type h that are used in subsystem S_i. The failure probability p_i of the ith subsystem is given by $p_i = \prod_{h\in S_i} q_h^{k_{ih}}$. Thus, from (1)

$$\hat{p}_{UB}(\tau) = \sum_{i=1}^{m}\left(\prod_{h\in S_i}\hat{q}_h^{k_{ih}}\right) - \sum_{(i,\,j)\,\in\,\tau}\left(\prod_{j\in S_{ij}}\hat{q}_h^{k_{ih}+k_{jh}}\right), \quad (8)$$

where $S_{ij} = S_i \bigcup S_j$. If the component failure estimates are independent, the mean of $\hat{p}_{UB}(\tau)$ is computed straightforwardly from (8) as

$$E\left[\hat{p}_{UB}(\tau)\right] = \sum_{i=1}^{m}\prod_{h\in S_i} E\left[\hat{q}_h^{k_{ih}}\right] - \sum_{(i,\,j)\in\tau}\prod_{j\in S_{ij}} E\left[\hat{q}_h^{k_{ih}+k_{jh}}\right].$$

Consider now the variance of the estimate in (8), which is required in the computation of the IBR estimate. In terms of the estimates $\hat{q}_j$,

$$\begin{aligned}\operatorname{var}\left[\hat{p}_{UB}(\tau)\right] = {} & \sum_{i=1}^{m}\sum_{j=1}^{m}\left(\prod_{h\in S_{ij}} E\left[\hat{q}_h^{k_{ih}+k_{jh}}\right] - \prod_{h\in S_{ij}} E\left[\hat{q}_h^{k_{ih}}\right]E\left[\hat{q}_h^{k_{jh}}\right]\right)\\ & -2\sum_{i=1}^{m}\sum_{(j,\,l)\,\in\,\tau}\left(\prod_{h\in S_{ijl}} E\left[\hat{q}_h^{k_{ih}+k_{jh}+k_{lh}}\right]\right.\\ & \left.\qquad - \prod_{h\in S_{ijl}} E\left[\hat{q}_h^{k_{ih}}\right]E\left[\hat{q}_h^{k_{jh}+k_{lh}}\right]\right)\\ & + \sum_{(i,\,n)\,\in\,\tau}\sum_{(j,\,l)\,\in\,\tau}\left(\prod_{h\in S_{injl}} E\left[\hat{q}_h^{k_{ih}+k_{nh}+k_{jh}+k_{lh}}\right]\right.\\ & \left.\qquad - \prod_{h\in S_{injl}} E\left[\hat{q}_h^{k_{ih}+k_{nh}}\right]E\left[\hat{q}_h^{k_{jh}+k_{lh}}\right]\right),\end{aligned}$$

where $S_{ijl} = S_{ij} \bigcup S_l$ and $S_{injl} = S_{inj} \bigcup S_l$. The equation for the variance is an extension of the variance expression in [18] to upper bound estimates in (1). As with computation of the mean of $\hat{p}_{UB}(\tau)$, the variance can be obtained in terms of the higher order moments of $\hat{q}_j$.

V. EXAMPLE

We illustrate the application of IBR for estimating system probability of failure on a military aircraft system. The example and data come from [19]. The aircraft system consists of nine subsystems that must function for the system to deliver an air-to-air missile. The subsystems include: flight structures, avionics, power, flight control, environmental, acquisition/fire control, launching, missile interface, and human intervention. Let S denote the entire system and $S_1,\ldots,S_9$ denote the nine subsystems. The test data and failure probability of each subsystem (obtained from [19]) is listed in Table 1. Aircraft system level testing resulted in 14 failures in 205 tests giving the estimate of failure probability and variance $\hat{p} = 0.068$ and $\hat{\sigma} = 0.018$, respectively.

To form the IBR estimate, the variance of the failure probabilities must be computed. For the three subsystems that do not have any observed failures, the test data is augmented to include an additional test that is a failure (see Section 3.4). Adding the additional fictitious test does not

TABLE 1.
SUBSYSTEM RELIABILITY TEST DATA AND ESTIMATES

Subsystem S_i	Number of Tests	Number of Failures	Failure Probability Estimate $\hat{p}_i$
1	130	1	0.008
2	130	0	0.000
3	130	1	0.008
4	130	1	0.008
5	130	0	0.000
6	250	3	0.012
7	130	1	0.008
8	250	1	0.004
9	330	0	0.000

alter the interpretation of the upper bound estimate; with the additional tests the upper bound estimate is more conservative. Using the augmented test data the estimate of the Bonferroni upper bound and standard deviation are $\hat{p}_{UB} = 0.065$ and $\sigma_{UB} = 0.021$, respectively. The estimate of the optimal weighting is $\hat{\lambda}^* = 0.576$; the IBR method is giving more weight to the full system estimate because its variance is smaller. The IBR estimate (an upper bound on the system reliability) is $p_{\hat{\lambda}^*} = 0.067$ and the 90% upper confidence limit on the estimate is 0.084.

The IBR estimate of the system reliability can be improved by including joint subsystem failure data. To illustrate this property we deviate from the example in [19]. We assume that failures in the avionics and power subsystems are highly correlated. Also, we assume that the systems are tested jointly 130 times and one joint failure is observed. By modifying the Worsley Bound, (4), so that only one joint probability is needed, the additional test data can be used to improve the IBR estimate. The new estimate of the upper lower bound and standard deviation are $\hat{p}_{UB} = 0.057$ and $\sigma_{UB} = 0.022$, respectively. The estimate of the optimal weighting is $\hat{\lambda}^* = 0.608$; the IBR method gives even more weight to the full system estimate because the lower bound standard deviation has increased from the example above. The new IBR estimate is $p_{\hat{\lambda}^*} = 0.064$ and the 90% upper confidence limit on the estimate is 0.082.

VI. CLOSURE

We describe above the IBR-based approach to estimating the reliability of complex system. The IBR method offers some convenient statistical properties while allowing for the use of full subsystem and subsystem test data to bound the estimate of the system reliability.

REFERENCES

[1] Baxter, L. (1993), "Towards a Theory of Confidence Intervals for System Reliability," *Statistics and Probability Letters*, vol. 16, pp. 29–38.

[2] Boland, P. J., Proschan, F., and Tong, Y.L. (1993), "Some Recent Applications of Stochastic Inequalities in System Reliability Theory," *Advances in Reliability*, pp. 29–41, A. P. Basu, ed., Elsevier, pp. 29–41.

[3] Hwang, C.L., Tillman, F.A., and Lee, M.H. (1981), "System-Reliability Evaluation Techniques for Complex/Large Systems—A Review," *IEEE Transactions on Reliability*, vol. R-30, pp. 416–423.

[4] Spall, J. C. (2010). "Convergence analysis for maximum likelihood-based reliability estimation from subsystem and full system tests." In *Proceedings of the 49th IEEE Conference on Decision and Control*, Atlanta, GA, 15−17 December 2010, pp. 2017−2022 (paper WeC09.2).

[5] Maranzano, C. J. and Spall, J. C. (2010). "Robust test design for reliability estimation with modeling error when combining full system and subsystem tests." In *Proceedings of the American Control Conference*, number ThB17.6, pages 3741–3746, Baltimore, MD, June–July 2010.

[6] Hunter, D. (1976), "An Upper Bound for the Probability of a Union," *Journal of Applied Probability*, vol 13, pp. 597-603.

[7] Worsley, K.J. (1982), "An Improved Bonferroni Inequality and Applications," *Biometrika*, vol. 69, pp. 297–302.

[8] Naiman, D. Q. and Wynn, H.P. (1997), "Abstract Tubes, Improved Inclusion-Exclusion Identities and Inequalities, and Importance Sampling," Annals of Statistics, vol. 25, pp. 1954–1983.

[9] Kwerel, S.M. (1975), "Most Stringent Bounds on Aggregated Probabilities of Partially Specified Dependent Systems," *Journal of the American Statistical Association*, vol. 70, pp. 472–479.

[10] Kounias, E. (1968), "Bounds for the Probability of a Union, with Applications," *The Annals of Mathematical Statistics*, vol. 39, pp. 2154–2158.

[11] Parkinson, D. B. (1988), "Reliability Bounds for Dependent Failures," *IEEE Transactions on Reliability*, vol. 37, no.1, pp. 54–56.

[12] Isermann, R. (1984), "Process Fault Detection Based on Modeling and Estimation Methods–A Survey," *Automatica*, vol. 20, pp. 387–404.

[13] Kerr, T. (1987), "Decentralized Filtering and Redundancy Management for Multisensor Navigation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-23, pp. 83–119.

[14] Spall, J. C. (1988), "Bayesian Error Isolation for Models of Large-Scale Systems," *IEEE Trans. Automatic Contr.*, vol. 33, pp. 341–347.

[15] Maryak, J. L. and Asher, M. A. (1993), "Isolating Errors in Models of Complex Systems," *IEEE Trans. Aerosp. Electron. Syst.,* vol. 29, pp. 452–463.

[16] Maranzano, C. J. (2008), "Using the Inequality-Based Reliability Method to Estimate the Reliability of Complex Systems," *Proceedings of the 2008 AIAA Missile Science Conference*, November 2008, Monterey, CA, Session 10-MS-10.

[17] Myhre, J. M. and Saunders, S. C. (1968), "Comparison of Two Methods of Obtaining Approximate Confidence Intervals for System Reliability," *Technometrics*, vol. 10, no. 1, pp. 37–49.

[18] Jin, T. and Coit, D. (2001), "Variance of System-Reliability Estimates With Arbitrarily Repeated Components," *IEEE Transactions on Reliability*, vol. 50, no. 4, pp. 409–413.

[19] Martz, H. F., Waller, R. A., and Fickas, E. T. (1998), "Bayesian Reliability Analysis of Series Systems of Binomial Subsystems and Components," *Technometrics*, vol. 30, pp. 143–154.