Stochastic Reliability Analysis: The Interface for Component Data Evaluation

Peter Dörre
SIEMENS AG (KWU), Offenbach, FRG

INTRODUCTION

It is well known that the so-called "independent failure" analysis can produce meaningless results for redundancy structures. Apart from exhausting possibilities of modelling e. g. shared components explicitly, to date the preferred solution to overcome this drawback is to apply parametric common cause failure (CCF) models. Recently an alternative class of approaches has been proposed (Hughes, 1987; Dörre, 1989). This type of stochastic approach allows to elicit definitions, concepts and models of conventional CCF analysis (Dörre, 1989).

This paper reviews the generalized Binomial distribution model for the reliability analysis of redundancy structures. Furthermore, procedures for data evaluation in order to determine the parameters of this approach are proposed.

CONCEPTS AND BASIC EQUATIONS OF STOCHASTIC RELIABILITY ANALYSIS

The basic concept of stochastic reliability analysis (SRA) is linked to a probability density function (PDF) which describes the *objective variability* of the failure behaviour of a component with respect to its existence in different environments (i. e. the component's subjection to different boundary conditions with respect to design, installation, operation, test and maintenance, physical environment) which coexist in a given statistical population. This variability is manifested by different failure frequencies, although there is often few or no knowledge on the detailed causes or mechanisms leading to the differences.

If there were only one environment, the resulting homogeneous failure behaviour could be described by a quantity without variability (yet with uncertainty with respect to its "true" value). Generally there is more than one possible environment or type of failure behaviour. As a component is always in exactly one environment, different environments do not interact (which establishes conditional independence). If there is more than one environment, the use of a model which considers only one failure behaviour corresponds to an averaging process over the population, leading to the creation of one "average" environment.

To proceed, the relative failure frequency (e. g. per test demand of a standby system) is considered as a "physical observable" X which describes the failure process. The spectrum of "eigenvalues" of this random variable in a non-homogeneous population (a mixture of different failure behaviours) is defined by the failure "probabilities" p_i, which occur with relative frequencies $a_i = Pr(X=p_i)$ for the i-th environment, i. e. $\sum_i a_i = 1$, and is described by the discrete PDF

$$f(x) = \sum_i a_i \, \delta(x-p_i) \qquad (1)$$

where δ is Dirac's delta function. These parameters may further be *subjectively uncertain*. This different feature is not addressed here.

Perfect redundancy is equivalent to the situation that all redundant components are in the same environment, i. e. one component is "multiplied". The failure of exactly r of k redundant components is then given by

$$P_{r/k} = \int b(r,k|x)\ f(x)\ dx \qquad (2)$$

with the Binomial term

$$b(r,k|x) = \binom{k}{r}\ x^r\ (1-x)^{k-r} \qquad (3)$$

With the discrete PDF of eq 1, the *generalized Binomial distribution model* is obtained, which for the single and multiple failure event frequencies yields

$$P_{r/k} = \binom{k}{r} \sum_i a_i\ p_i^r\ (1-p_i)^{k-r} \qquad (4)$$

Independent failure. The independent failure approach corresponds to choosing a quasi-deterministic single-point approximation for the PDF, i. e.

$$\bar{f}(x) = \delta(x-\bar{p}) \qquad (5)$$

The only parameter of this degenerate PDF is given by the expected value or first (central) moment of the original PDF (eq 1)

$$\bar{p} = \langle x \rangle = \int x\ f(x)\ dx = \sum_i a_i\ p_i = P_{1/1} \qquad (6)$$

In this oversimplified approach an approximation $\bar{P}_{r/k}$ for $P_{r/k}$ is calculated by

$$\bar{P}_{r/k} = \binom{k}{r}\ \bar{p}^r\ (1-\bar{p})^{k-r} \qquad (7)$$

It is well-known from stochastic calculus that e. g. the n-th moment $\langle x^n \rangle$ of a PDF is never less than the n-th power of the first moment, $\langle x \rangle^n$,

$$\langle x^n \rangle = \sum_i a_i\ p_i^n \geq \left(\sum_i a_i\ p_i\right)^n = \langle x \rangle^n \qquad (8)$$

which is a special case of Ljapunov's inequality. Equivalence here only holds when the degenerate PDF (eq 5) is used, i. e. in the independent failure case.

Perfect diversity is equivalent to the situation that the environments of the redundant and diverse components are not coupled, i. e. the averaging procedure can be carried out independently for each redundancy. (Realistic diversity can be considered as a measure of the degree of imperfection in redundancy.) Hence for non-redundant as well as for perfectly diverse structures, both the general PDF (eq 1) and the simplified PDF for "independent failure" (eq 5) fortuitiously lead to the same result. However, when for redundant structures the stochastically inconsistent method (eq 7) is used, it is not astonishing that the obtained results are usually poor, especially for higher degrees of redundancy.

With the increase in available data on multiple failure events this discrepancy has become obvious from operational experience. To meet this issue, a subsequent "CCF" treatment to generate agreement between theory and reality is usually considered as the panacea. Fundamental disadvantages of this "practical" approach are the "explosion" of the number of minimal cutsets caused by the explicit representation of CCF terms in the logic model (Mosleh et al, 1988) and the dissemination of a stochastically inconsistent approximation which violates the rule that averaging is the *last* step in a stochastic calculation. The latter feature can be considered as the reason for the vagueness and the lack of a

convincing definition of the "CCF" concept as a whole. The alternative approach is to work in the stochastically consistent picture from the beginning, which ultimately excludes the need for any further "CCF" correction (Dörre, 1989).

These remarks address the CCF concept as a tool for quantitative calculation: I do not doubt its usefulness for other purposes, e. g. for system design on a comparative or qualitative level, although in my opinion the better approach should be preferably based on a concept with at least two orthogonal features defined by incomplete resp. complete redundancy, or coherent (coupled) failure versus incoherent failure, the latter referring to the range from perfect redundancy to perfect diversity.

THE SERIES OF GENERALIZED BINOMIAL DISTRIBUTION MODELS

The number of shells considered in the PDF determines the special model.

Coherent failure. While eq 5 defines the (degenerate) PDF for independent failure, the simplest model for perfectly dependent failure (the "coherent failure" or "no redundancy/multiplicity" case) is defined with $a_0 > 0$ by

$$f(x) = a_0\ \delta(x-1) + (1-a_0)\ \delta(x-0) \qquad (9)$$

$$P_{r/k} = \begin{cases} a_0, & r=k \\ 0, & 0<r<k \\ 1-a_0, & r=0 \text{ (intact state)} \end{cases} \qquad (10)$$

Coherent and independent failure. The simplest extension of the trivial PDFs (eqs 5 and 9) requires 2 parameters:

$$f(x) = a_0\ \delta(x-1) + (1-a_0)\ \delta(x-p_1) \qquad (11)$$

which e. g. yields for a 2-redundant structure

$$P_{2/2} = a_0 + (1-a_0)\ p_1^2 \qquad (12)$$

It has been shown (Dörre, 1989) that this expression is equivalent to the exact equation for double failure in the ß-factor model, with its two parameters ß and Q (= total component failure probability) set to

$$\begin{aligned} ß &= a_0/(a_0+p_1) \\ Q &= a_0+p_1 \end{aligned} \qquad (13)$$

Simplest general case. The simplest sufficiently flexible approximation for higher degrees of redundancy involves 3 shells (Dörre, 1989)

$$f(x) = a_0\ \delta(x-1) + a_1\ \delta(x-p_1) + (1-a_0-a_1)\ \delta(x-p_2) \qquad (14)$$

This is a model with *four* parameters. Apart from the "lethal shock" or "coherent failure" shell given by a_0 and $p_0 = 1$, which only contributes to the "total system" failure frequency $P_{k/k}$, all other shells contribute to *all* multiplicities in failure. In contrast to Hughes (1987), it is therefore concluded that the fact of multiple failure alone is not an appropriate identifier for an environment (described by a delta shell).

In the generalized Binomial distribution model, no parameter describes failure of o*nly one* redundancy, as is e. g. the case in the Binomial failure rate (BFR) model with lethal shock (cf. Apostolakis and Moieni, 1987). Beyond *formal* similarity, corresponding parameters of the two models have different meanings.

Although it is in principle possible to define a three-parameter (two-shell) model, all models with an *odd* number of parameters either do not account for the "lethal shock" environment adequately or have a dependent or dummy parameter. I finally note that due to the *sum rules* which hold for the a_i's and the $P_{r/k}$'s, one can determine exactly k "free" parameters from multiple failure events (including single and no failure) in k-redundant structures.

DETERMINATION OF MODEL PARAMETERS FOR SPECIAL APPLICATIONS

At least for i>0, the parameter set (p_i, a_i) can be determined directly from operational experience on different component types fulfilling the same function (e. g. different auxiliary feedwater pumps), taking into account plant-to-plant variability due to different manufacturer types, operational conditions, test/maintenance strategies etc. Such information is also contained in records of repeated individual failure or of enhanced single failure for specified subpopulations. Such data are not evaluated within the CCF picture. The *new requirement for data evaluation* therefore is to focus on how often (a_i) subpopulations with *deviations* from an expected "generic" value (especially with enhanced p_i's) exist. Engineering judgment is needed to decide how the weights a_i determined from past operational experience have to be modified for a new application, e. g. the reliability prediction for a system under design.

Alternatively, the set of SRA model parameters can be calculated in the conventional way from usually rare multiple failure events. Here each event has to be assessed with respect to its relevance for the application, accounting for differences relative to the data source system; the result can be conveniently represented by an *impact vector*, as described in Mosleh et al (1988). The solution for the two-parameter model can be obtained by inverting eq 13 (Dörre, 1989). The solution for the generalized Binomial distribution model with at least four parameters is given in what follows.

PRELIMINARY DATA EXCHANGE WITH THE BASIC PARAMETER MODEL

In this section the data compatibility of the SRA approach with respect to already available data for multiple failure events collected in "CCF" contexts is investigated. Such data can e. g. be represented by the parameters of the basic parameter (BP) model, the "parent" model of many other parametric CCF models (Mosleh et al, 1988), i. e. by the relative event frequencies

$$Q_r^{(k)} = n_r^{(k)} / (\binom{k}{r} N_D) \qquad (15)$$

Here $n_r^{(k)}$ is the absolute number of exactly r of k (for r>1 dependent) multiple failure events, and N_D the number of system demands.

For a 4-redundant structure, it can be shown that the total system failure frequency $P_{4/4}$ is given by (the superscript "(4)" is suppressed for convenience)

$$P_{4/4} = Q_4 + 4\,Q_3\,Q_1 + 3\,Q_2^2 + 6\,Q_2\,Q_1^2 + Q_1^4 + 6\,Q_3^2 + 12\,Q_3\,Q_2 + 4\,Q_2^3 + 12\,Q_2^2\,Q_1 \qquad (16)$$

In the generalized Binomial distribution model of SRA, the same frequency is given by the fourth (central) moment of the PDF, i. e.

$$P_{4/4} = m_4 = \langle x^4 \rangle = \sum_i a_i\, p_i^4 \qquad (17)$$

The 3-shell approximation of the PDF (eq 14) then requires the determination of the 4 "free" parameters a_0, a_1, p_1, p_2 as functions of Q_r, r = 1 to 4. It can now be recognized that the first line of the right-hand side of eq 16 is the *cumulant representation* of the fourth moment (Müller, 1975)

$$m_4 = c_4 + 4\,c_3\,c_1 + 3\,c_2^2 + 6\,c_2\,c_1^2 + c_1^4 \qquad (18)$$

whereas the second line stems from the CCF logic model development (Mosleh et al, 1988) which formally creates such highly artificial terms with "overlapping" CCFs (these terms imply failure of a component by two or even more simultaneous common causes). If one disregards this feature, one clearly sees the correspondence between basic parameters and cumulants, $Q_r \langle\text{-}\rangle c_r$. The cumulants c_r can be calculated for any given PDF in terms of moments and hence in terms of (p_i, a_i)

$$c_1 = m_1 = \langle x \rangle = \sum_i a_i\,p_i \qquad (19)$$

$$c_2 = m_2 - m_1^2 = \langle x^2 \rangle - \langle x \rangle^2 = \sum_i a_i\,p_i^2 - \left(\sum_i a_i\,p_i\right)^2 \qquad (20)$$

$$c_3 = m_3 - 3\,m_2\,m_1 + 2\,m_1^3 \qquad (21)$$

$$c_4 = m_4 - 4\,m_3\,m_1 - 3\,m_2^2 + 12\,m_2\,m_1^2 - 6\,m_1^4 \qquad (22)$$

If the basic parameters were derived within an *empirical* interpretation of multiple failure events (i. e. without discrimination between "independent" and "common cause" failure), they would be equal to the "Binomial" moments

$$Q_r^{(k)} = m_r^{(k)} = \langle x^r\,(1-x)^{k-r} \rangle = \sum_i a_i\,p_i^r\,(1-p_i)^{k-r} \qquad (23)$$

To conclude, it has been demonstrated that the parameters of the generalized Binomial distribution model of SRA can be determined from available parameters of the BP model. This was shown for a 4-redundant structure, as a minimum of 4 parameters is both required and available for this degree of redundancy in the SRA model. In contrast to the SRA model, the BP model is redundancy-dependent. Therefore, "mapping up/mapping down" techniques (Dörre, 1987; Mosleh et al, 1988) are needed in order to compensate redundancy mismatch in an adequate way.

DETERMINATION OF THE LETHAL SHOCK PARAMETER

The major problem seems to be the determination of a_0, which defines the lower bound of the "total system" (k of k) failure frequencies. Here an iterative solution is proposed which uses operational experience as well as expert opinion.

1. Use definite knowledge from operational experience in the following way: incomplete multiple component failure (r of k components with r<k) is always evidence for the *exclusion* of a lethal shock environment. Any successful test of a single component from a redundant structure (e. g. by staggered testing) is a sufficient sample (counter-example) against the hypothesis of a "total system" CCF. Here knowledge of *success* information, i. e. how many of the redundant components did *not* fail in an event, is essential.

2. The following logic property is accounted for: complete (k of k) multiple component failure is a *necessary*, but not a *sufficient* condition for the verification of the assumption "lethal shock environment", as all other environments also contribute to this event. A proof of the sufficiency condition requires to exclude that the failure is due to non-lethal environments. Further engineering judgment is necessary in this case. It is clear that any other knowledge about the special circumstances of the failure event has to be accounted for additionally if available. For example, multiple incipient failure can rarely be caused by a lethal shock, but is rather due to
   - an enhanced failure probability or
   - a failure rate growing (perhaps unexpectedly) with time.

The requirement that multiple failures occur simultaneously (or less strict: in a short time interval) known from the "classical" CCF picture remains valid for lethal shocks resp. coherent failure.

3. Further improvement can be obtained by accounting for the degree of belief (certainty) associated with the degree of redundancy, especially when the special circumstances of the case are not sufficiently known: it is e. g. more likely that a 4 of 4 failure is due to a "lethal shock" than a 2 of 2 failure. While the case r=k=1 is uninformative, the degree of belief that such an event is due to lethal shock increases with increasing k and approaches certainty for $k \to \infty$.

CONCLUSIONS AND RECOMMENDATIONS

SRA is a consistent tool to model dependent failure. While Hughes (1987) called this concept a new approach to CCF, I would prefer to speak of an *old* approach: the concept of "ensemble averaging" is a 19th-century achievement of statistical physics. Hence there is no point in challenging it in terms of plausibility, practicability, credibility etc. which seem to be the predominant design gaols for contemporary CCF models. This concept has been introduced into reliability analysis in order to remove the largely ficticious "corrective" picture of CCF which was used for bridging the gap between reality and the results from the oversimplified theory of "independent failure". The gap is created by ignoring or "averaging out" population variability, not by the existence of an extra phenomenon related to common causes.

It is further shown how one can use available data on dependent failure events to determine preliminary parameter values for the generalized Binomial distribution model, thus compensating a possible initial (complaint about) lack of data collected in the frame of (and hence readily available for) SRA. For future data collection activities, this frame is recommended only as a starting point: in addition, *data on variability* have to be evaluated extensively.

The determination of the "lethal shock" parameter a_0 can be supported by expert judgment: the evaluation of qualitative features of failure events and of their value as statistical evidence within the logical concept of necessary and sufficient conditions. How a sufficient condition can be specified for the identification of a "lethal shock" environment needs further investigation.

REFERENCES

Apostolakis, G., and Moieni, P. (1987). The Foundation of Models of Dependence in Probabilistic Safety Assessment. Reliab. Engng. 18, pp. 177-195

Dörre, P. (1987). Possible Pitfalls in CCF Data Evaluation. Proc. of the 9th Int. Topical Conf. on Probabilistic Safety Assessment and Risk Management (PSA '87), Zurich, Switzerland, Aug. 31-Sept. 4, 1987, Vol. 1, Verlag TÜV Rheinland GmbH, Köln, pp. 31-36

Dörre, P. (1989). Basic Aspects of Stochastic Reliability Analysis. Reliab. Engng. and System Safety 24, pp. 92-116

Hughes, R. P. (1987). A New Approach to Common Cause Failure. Reliab. Engng. 17, pp. 211-236

Mosleh, A., Fleming, K., Parry, G., Paula, H., Worledge, D., and Rasmuson, D. (1988). Procedures for Treating Common Cause Failures in Safety and Reliability Studies, Procedural Framework and Examples. NUREG/CR-4780 (PLG-0547), Vol. 1, US Nuclear Regulatory Commission, Washington

Müller, P. H. (ed.) (1975). Lexikon der Stochastik, 2nd edition, Wissenschaftliche Buchgesellschaft, Darmstadt