The Concept of Dependence in PSA

George E. Apostolakis
University of California, Los Angeles, CA USA

1 INTRODUCTION

The issue of dependence of uncertain quantities has always been recognized as one of major importance in probabilistic safety analysis (PSA). In particular, dependent failures (or common-cause failures (CCF)) are a subject of continuing interest and investigation, since it has been widely accepted that the coincident independent failures of components are, in general, a minor contributor to system unavailability and unreliability.

The various kinds of dependence that have been identified frequently cause a conceptual confusion as to what exactly they represent. There is a tendency, for example, to treat all kinds of dependence as part of a CCF analysis. That this, in fact, is not true is part of what we intend to show in this paper. We will make a clear distinction between stochastic and state-of-knowledge dependences.

The intellectual foundations of our investigation are in the subjectivistic approach to the theory of probability, as formulated by De Finetti (De Finetti, 1974).

2 THE STOCHASTIC MODEL

To make the discussion concrete and without substantive loss of generality we will assume that we have to model the coincident unavailability at a given moment of two components A and B (these could be, for example, a minimal cut set of a fault tree). Let $X_j, j = A,B$, be the indicator variables associated with these components, i.e.,

$$X_j = \begin{cases} 1, & \text{if component } j \text{ is down,} \\ 0, & \text{otherwise,} \end{cases}$$

$$j = A \text{ or } B.$$

The indicator variable for the system of two components is, then,

$$X_s = X_A X_B. \tag{1}$$

We now define the unavailabilty of A as

$$\phi_A \equiv fr(X_A = 1) \tag{2}$$

with the following interpretation. If we were to perform a thought experiment in which there were very many systems identical to S and under identical conditions, then ϕ_A would be the fraction of these systems in which A happens to be unavailable at the given instant regardless of the status of B. The choice of notation in eq. (2) is, then, evident. We can similarly define ϕ_B.

We note that these definitions are relative-frequency based. However, we do not use the term "probability", as it is often done, because we wish to reserve this term for degrees of belief. At this point of the evolution of the state of the art it is important to be very careful in our terminology. Kaplan and Garrick (Kaplan and Garrick, 1981) are very careful, in defining the concept of risk, to distinguish between "probability" and "frequency". The latter is, of course, the unavailability (the "fraction") that we defined above. We shall try to keep these concepts separate "perhaps even too insistently, with the risk, and near certainty, of irritating the reader", as De Finetti puts it, when he comments on "the tyranny of language" in his definitive book (De Finetti, 1974).

We can now consider two interesting cases.

2.1 Conditional Stochastic Independence

When the components A and B are of different kind, e.g., a pump and a valve, and well separated, so as not to be susceptible to extreme common environments, it is reasonable to assume that they fail independently. Then we write

$$fr(X_j = 1|\phi_A,\phi_B) = \phi_j, \qquad j = A,B, \tag{3}$$

$$fr(X_s = 1|\phi_A,\phi_B) = \phi_A\phi_B. \tag{4}$$

Equations (3) and (4) show explicitly that the unavailabilities of the components and the system are given in terms of ϕ_A and ϕ_B, which are assumed to be known. To calculate the unconditional system and component unavailabilities we need to remove this condition, as we will show later.

2.2 Conditional Stochastic Dependence

In a typical case of redundant safety systems, A and B are nominally identical components that are susceptible to failure due to some common cause. Building models that capture these dependencies is the subject of CCF analysis (Vesely, 1977; Fleming et al, 1986; Apostolakis and Moieni,1986). A simple model consists of three parameters (Moieni and Apostolakis, 1983; Dinsmore and Pörn, 1986):

ϕ_0: the fraction of times (demands) in which neither component fails;

ϕ_1: the fraction of times in which exactly one component fails;

ϕ_2: the fraction of times in which both components fail;

$\phi_0 + \phi_1 + \phi_2 = 1.$

Then, the conditional unavailability of the system is

$$fr(X_s = 1|\phi_0,\phi_1,\phi_2) = \phi_2 \tag{5}$$

(more elaborate expressions can be produced, if more failure causes are considered (Moieni and Apostolakis, 1983). The reason for our terminology is, again, evident in eq. (5), namely, the model assumes knowledge of the three parameters ϕ_0, ϕ_1 and ϕ_2.

The component unavailabilities can also be expressed as functions of these parameters, i.e.,

(6) $$fr(X_A = 1|\phi_0,\phi_1,\phi_2) = \phi_1 + \phi_2,$$

(7) $$fr(X_B = 1|\phi_0,\phi_1,\phi_2) = \phi_1 + \phi_2.$$

3 PROBABILITY

The numerical values of the parameters of the stochastic models that we have discussed can be thought of as representing different hypotheses about the conditions of failure of the components. For example, a high value for ϕ_2 may suggest that the components are operating in an environment in which common extreme conditions are likely to occur. It is our current state of knowledge that dictates how likely each of these hypotheses is. This state of knowledge is expressed numerically by probability distributions. Thus for the model of eqs. (3) and (4) we need the joint probability density function (pdf) of ϕ_A and ϕ_B, say $\pi(\phi_A,\phi_B)$. Similarly, for the models of eqs. (5)-(7) we need the pdf $\pi(\phi_0,\phi_1,\phi_2)$.

The unconditional unavailabilities for the components (q_A and q_B) and for the system (Q_S) can now be readily calculated.

Thus for the model of stochastic independence we have

(8) $$q_j = \iint d\phi_A d\phi_B \pi(\phi_A,\phi_B)\phi_j, \qquad j = A,B,$$

(9) $$Q_s = \iint d\phi_A d\phi_B \pi(\phi_A,\phi_B)\phi_A\phi_B$$

and, for the model of stochastic dependence,

(10) $$Q_s = \iiint d\phi_0 d\phi_1 d\phi_2 \pi(\phi_0,\phi_1,\phi_2)\phi_2,$$

(11) $$q_B = q_A = \iiint d\phi_0 d\phi_1 d\phi_2 \pi(\phi_0,\phi_1,\phi_2)(\phi_1 + \phi_2).$$

The general situation is now clear. We first construct a conditional stochastic model that models the physical behaviour of the system. This could range from the simple exponential law for the failure of a single component, i.e.,

(12) $$f(t|\lambda) = \lambda \exp[-\lambda t],$$

to a complete PSA that utilizes event and fault trees. The result of this stochastic model is, in general, an expression that depends on a set of parameters $\underline{\phi} \equiv (\phi_1,\phi_2, \ldots, \phi_N)$, i.e.

$$fr(X_s = 1|\underline{\phi}),$$

where $X_S = 1$ represents the event of interest.

Our state of knowledge concerning the numerical values of $\underline{\phi}$ (the different "hypotheses" of the stochastic model) is expressed by the pdf $\pi(\phi)$. Then, the unconditional system characteristic (that is represented by the event $X_S = 1$) is

(13) $$Q_s = \int d\underline{\phi} \pi(\underline{\phi}) fr(X_s = 1|\underline{\phi})$$

(just to complete the almost trivial example of eq. (12), the Reactor Safety Study (RSS) (WASH-1400, 1975) has established the practice of using lognormal distributions for $\pi(\lambda)$).

The state-of-knowledge (sok) pdf $\pi(\underline{\phi})$ must be determined by carefully examining what we know (and how we came to know it) about the parameters $\underline{\phi}$. Two examples will clarify what we mean.

When the components are nominally identical, we write

$$\pi(\phi_A,\phi_B) = \pi(\phi_A)\delta(\phi_B-\phi_A), \tag{14}$$

where $\delta(\phi_B-\phi_A)$ is the delta-function.

Then, eq. (9) becomes

$$Q_s = \int d\phi_A \pi(\phi_A)\phi_A^2 \tag{15}$$

which also indicates that eq. (4) should be written as

$$fr(X_s = 1|\phi_A,\phi_B) = \phi_A^2. \tag{16}$$

The fact that eq. (16) should be used in lieu of eq. (4) when the components are nominally identical has been discussed by Apostolakis and Kaplan (Apostolakis and Kaplan, 1981). It is an interesting example, because it has uncovered some of the misunderstandings that exist among PSA practitioners.

This "failure rate coupling", as it is sometimes referred to, has been used as another CCF model. Our present discussion, of course, shows that this is erroneous. In fact, eqs. (15) and (16) indicate that the components are (conditionally) stochastically independent, i.e., no coupling of the failures has been introduced. However, because the individual unavailabilities are the results of the same body of knowledge, there is complete dependence at the sok level. We also note that the components are unconditionally dependent. This is easily seen, when we compute the individual unconditional unavailabilities using eqs. (8) and (14), i.e.,

$$q_j = \int d\phi_A \pi(\phi_A)\phi_A, \qquad j = A,B. \tag{17}$$

Then, it is clear from eqs. (15) and (17) that

$$Q_s \neq q_A q_B, \tag{18}$$

that is, the unavailabilities are, indeed, unconditionally dependent.

A numerical example demonstrating the importance of these developments is taken from the Zion PSA (Pickard, Lowe and Garrick, Inc., 1981). The failure mode of interest is the joint failure (due to rupture) of two motor-operated valves which are in series in the residual heat removal (RHR) suction path (commonly called the V sequence or interfacing systems loss-of-coolant accident).

It is straightforward to verify that (18) is true. We can calculate Q_s from eq. (15). However, it is simpler to recognize that Q_s is the mean value of ϕ_A^2 and can be obtained as

$$Q_s = [\text{mean}(\phi_A)]^2 + \text{variance}\ (\phi_A). \tag{19}$$

It is given that

$$\text{mean}(\phi_A) = 1.17\cdot10^{-3}$$

(this is also q_A, eq. (17)) and

$$\text{variance}\ (\phi_A) = 8.29\cdot10^{-6}.$$

Thus

$$Q_s = 9.66\cdot10^{-6}, \tag{20}$$

which differs from the product $q_A q_B$ ($1.37 \cdot 10^{-6}$) by the value of the variance of ϕ_A, i.e., $8.29 \cdot 10^{-6}$. In this particular case the distribution of ϕ_A is broad enough, so that this variance makes a significant difference in the result. Therefore, if the sok dependence had been ignored, the frequency of the V sequence would have been underestimated by a factor of almost 7 ($9.66 \cdot 10^{-6}$ vs. $1.37 \cdot 10^{-6}$).

The sok distribution $\pi(\phi_0,\phi_1,\phi_2)$ of the model of stochastic dependence that we discussed earlier, eqs. (5)-(7) and (10), (11), can be one of the available multivariate distributions, e.g., the Dirichlet or lognormal distributions. For example, the Dirichlet distribution in our case is

$$\pi(\phi_0,\phi_1,\phi_2) = C\phi_0^{\alpha_0}\phi_1^{\alpha_1}\phi_2^{\alpha_2}, \tag{21}$$

where C is a normalizing constant. This form of distribution requires that we quantify our knowledge concerning the numerical values of ϕ_0, ϕ_1 and ϕ_2 simultaneously, which is reasonable (and, in fact, mandatory), since these three quantities are the relative frequencies of the three mutually exclusive and exhaustive states of the redundant system (see sect. 2). In other words, what we know about ϕ_2 is correlated to what we know about ϕ_0 and ϕ_1 and, thus, the corresponding distributions cannot be assessed independently, as it is often done in such cases in practice.

A major problem associated with eq. (21) is the assessment of the parameters α_0, α_1 and α_2. Analysts, in general, have difficulties in producing sok distributions for single variables (Apostolakis, 1986), thus, in our case of three variables, this becomes an almost impossible task. However, when statistical evidence is available and the knowledge prior to this evidence is vague, Bayes' theorem can be employed to produce an appropriate sok distribution, as it will be shown in the next section.

REFERENCES

Apostolakis, G. (1986). Nucl. Eng. Des., Vol. 93, p. 161.

Apostolakis, G. and Kaplan, S. (1981). Reliab. Eng., Vol. 2, p. 135.

Apostolakis, G. and Moieni, P. (1986). In Reliability Data Collection and Use in Risk and Availability Assessment, edited by H. J. Wingender (Springer-Verlag, Heidelberg, Germany), p. 407.

De Finetti, B. (1974). Theory of Probability, Vol. 1 and 2 (John Wiley and Sons, New York, N.Y.).

Dinsmore, S. and Pörn, K. (1986). CCF quantification from plant data, Studsvik Energiteknik report NP-86, Nyköping, Sweden.

Fleming, K. N., Mosleh, A. and Deremer, R. K. (1986). Nucl. Eng. Des., Vol. 93, p. 245.

Kaplan, S. and Garrick, B. J. (1981). Risk Analysis, Vol. 1, p. 11.

Moieni, P. and Apostolakis, G. (1983). Transactions of the American Nuclear Society Winter Meeting, (American Nuclear Society, San Francisco, CA), Vol. 45, p. 387.

Pickard, Lowe and Garrick, Inc., Westinghouse Electric Corporation, Fauske and Associates, Inc. (1981). Zion Probabilistic Safety Study (Commonwealth Edison Co., Chicago, IL).

Vesely, W. E. (1977). In Nuclear Systems Reliability Engineering and Risk Assessment, edited by J. B. Fussell and G. R. Burdick (SIAM, Philadelphia, PA), p. 314.

WASH-1400, Reactor Safety Study, Appendix III (1975). Failure Data (US Nuclear Regulatory Commission, Washington, DC).