On Models for Causal Dependency

Gerath W. Parry
NUS Corporation, Gaithersburg, MD USA

INTRODUCTION

The numerous Probabilistic Safety Assessment (PSAs) that have been performed over the last few years have focussed attention on the importance of treating correctly the dependency between the events representing failures of redundant and diverse components of various systems. As briefly reviewed in the next section, although many sources of dependency are treated explicitly in the logical structure of the models (the event trees and fault trees), it has been found to be convenient to include, in these models, events that are called common-cause failure events. A recent NRC/EPRI document (Mosleh et al., 1988) presents a procedure for the identification and definition of these events, and for the quantification of their probabilities. Dorre (1989) has suggested that the introduction of the idea of common-cause failure as an additional phenomenon, to be treated with extra methods, is confusing, and has suggested an alternative approach to accounting for the experience data. This paper reviews some of the issues raised about the need for common-cause failure events in system models.

THE ORIGIN OF THE COMMON-CAUSE FAILURE CONCEPT

In constructing the logic models of PSAs, many causes of dependency are explicitly included in the structure of the model. For example, the failure of a motor operated pump is modeled as arising from failures of the pump itself, but also from failures of the power from the bus which supplies the motor. Further, the model of failure of the bus to supply power includes contributions from failures to supply power to the bus from both normal and emergency power supplies. Similarly, if the pump is such that it requires both direct, or room cooling, or both, failures of the cooling systems are modeled as potential failures of the pump. In this way, a model is constructed which reflects explicitly the hard-wired functional dependencies between the various components and systems of the plant.

The typical plant logic model, constructed in this way, models the plant response in terms of units called basic events, that represent particular failure modes of the components. Examples of such basic events are; pump A fails to start on demand, diesel generator D1 fails to run for 6 hours. To turn this model into a quantitative assessment tool, a probability model must be constructed which allows the evaluation of the probability of each basic event, preferably on the basis of some historical experience. The final stage in the quantification of the model is to specify the rules for combining the basic event probabilities and initiating event frequencies to obtain the accident sequence frequencies and system unavailabilities. The assumption of statistical independence of the basic events is an appealing

one to start with, but experience with collecting data on component failures has shown that the number of multiple coincidental failures of like components, compared with the number of single failure events, is higher than expected on the basis of that assumption. Hence, the concept of a common-cause model, to correct for this statistical dependence between the basic events, has been introduced. The interpretation and limitations of this CCF concept is discussed in the following sections.

CCF MODELS AND THEIR LIMITATIONS

The general approach to common-cause failure modeling, described in Mosleh et al., (1988) begins with the identification of common-cause component groups, i.e., those groups of components for which the independence assumption is suspected to be incorrect, and includes new basic events in the logic model which represent common cause failures of those groups and subsets of those groups. Then, for each new basic event, a probability model is constructed in exactly the same way as for the single component/failure mode basic events. The set of basic event probability models associated with the components in a common-cause component group is collectively known as a common-cause failure model.

The models discussed in Mosleh et al., (1988) generally have very little causal structure. With one exception they do not explain the relationship between single and multiple failure events, they merely recognize that such events can exist. The Basic Parameter Model defines the same type of probability model for each basic event of different multiplicity for components in a CCF group, e.g., a constant failure rate, or constant failure probability model, is assumed for the single, double, triple, etc., component failure basic events. The parameters of the basic event models are then free parameters to be fitted to the available data on the set of observed single, double, triple, etc., failure events. The Multiple Greek Letter, or Alpha Factor Method (and the more primitive Beta factor method) are reparameterizations of this model.

The Binomial Failure Rate Model does have an underlying causal picture in that it characterizes the role of agents, called shocks, in causing multiple failures. The probabilities of multiple failures are then prescribed on the basis of the frequency of the shocks, and according to whether the shocks are lethal (all components fail) or non-lethal where the number of components failed as a result of a non-lethal shock event is distributed binomially. The model has, at most, four parameters. The multinomial failure rate model also uses the concepts of independent and shock related failures, but the probabilities of multiple failure events are essentially free parameters.

These models, with the exception of the BFR, by definition have enough free parameters to fit any data; more free parameters are created as needed for higher redundancy systems. But, with the exception of the BFR, and even that only with specific assumptions, none of the models can be used to predict what changes in system availability a redundancy increase from 3 to 4 say, would result in. With the possible exception of the BFR model, they are not in any way theoretical models of the physics of failure, or characterizations of causal mechanisms. Their sole purpose is to guide an analyst in partitioning event data in a meaningful way, to enable him to estimate probabilities of failure events of varying multiplicity, which in the language of Mosleh et. al. (1988), are the basic events of the Basic Parameter Model. The creation of these basic events is an intermediate analysis step to bridge the gap between the algebraic (logical) solution to the system unavailability, expressed as component state cut-sets, and the quantification of that unavailability, can be regarded as a mathematical convenience to create quasi-independent basic events. (see the discussion in Appendix C of Mosleh et.al., 1989). However, if the process of common cause

failure analysis is to provide insights into plant behavior, it is important to understand the origin of the observed dependence.

CAUSES OF DEPENDENCE BETWEEN BASIC EVENTS

A basic event, whether it represents a single, or a multiple component failure, is in reality the logical sum of the events characterizing the occurrence of failure from the different mechanisms that can result in those failures. The common-cause failure interpretation is that the individual mechanisms have different potential for causing multiple failures, that is, the conditional probability of a second, third, etc., component failing given the first has failed from a particular cause is dependent on the cause. The picture that Dorre (1989) proposes is different in that it identifies different types of behavior with the occurrence of different environments. An environment has the effect of changing a component's failure rate, but within that environment, component failures are independent.

The different causes in the one model, or environments in the other, have different frequencies of occurrence. The probabilities of the basic events of standard reliability models then represent some sort of average behavior. In both of the conceptual models discussed above it can be shown that the probability of a multiple failure event cannot, except under particular limiting circumstances, be the appropriate power of the probability of a single component basic event defined in the traditional way. Thus, the need for the common-cause terms is a result of the definition of basic events to represent failure modes rather than failure causes or environments. However, while Dorre seems to be suggesting that at some lower level, that of the environment, component failure basic events may be defined as conditionally independent, the CCF picture still allows the possibility of additional dependence at the cause level. Further, it is clear that, in either case, it is essential to have a more complete understanding of failure mechanisms, which must come from a detailed analysis of the causes of multiple failure events.

CONSIDERATIONS IN THE ANALYSIS OF MULTIPLE FAILURE EVENTS

In order to analyze multiple failure mechanisms, the CCF analyst asks two questions; firstly, why and how do components fail, and secondly, what are the factors that result in more than one component having failed due to the same failure cause at the same time.

For this purpose, the description of a failure in terms of a single cause is too simplistic. For some purposes, it may be adequate to identify that a pump failed because of high humidity. But since we are interested in a detailed understanding of the potential for multiple failures we need to identify further why the humidity was high and why it affected the pump and whether is could affect other components. It is therefore important to describe failures as resulting from some chain of events.

For failures to become multiple failures, the conditions have to be conducive to all the components failing simultaneously., It is convenient to define a set of coupling factors. A coupling factor is a property of a group of components or piece parts that identifies them as susceptible to the same chain of events that can cause failure. Such factors include design, environment, maintenance and test procedures. They define the degree of common susceptibility and help define the common-cause component group. However, now it is important to identify how some element or elements of the chain of events can impact the components of the CCF group simultaneously. To a large extent this is equivalent to identifying how defenses against failures have failed.

Defenses against failures can be effective in many different ways. Firstly, they can operate to cure the symptoms of failure. An example would be to protect motor control centers against humidity by sealing them. This is eqivalent to hardening the component. Another example is the training of maintenance staff to assure correct interpretation of procedures. An approach to reduce multiple failures is to effectively decrease the similarity of these components and their environment in some way that prevents a particular type of root cause from affecting all components simultaneously, and allows more opportunity for detecting failures before they appear in all components of the group.

What is becoming clear from the research being sponsored by the NRC (Parry, et al.,) 1989), is that there are different classes of multiple failure mechanisms and that different models would be necessary to explicitly represent these mechanisms.

ACCOUNTING FOR CAUSAL MECHANISMS

In the procedure discussed in Mosleh et al.(1988), it is while analyzing event data that the issues concerning the causal mechanisms of failure and different failure behavior types are addressed. In particular, in analyzing multiple failure event data, a search is made for common elements in the chain of events that led to the failures, as these establish a causal dependence. It should be noted that the type of commonality that is looked for is a systematic factor which affects more than one component e.g., a single pipe break which causes a flood that affects more than one component, or a design error that affects all of the common-cause component group. The coincidence of failures from the same type of cause, but which does not arise from some single event in the causal chain is not sufficient to define it as a dependent event. For the conversion of generic to pseudo plant-specific data, this interpretation is essential so that the analyst can judge whether the causal mechanism seen at another plant is appropriate for his particular plant of interest. The analysis does lead to a recognition of different types of failure behavior, but no attempt is made to characterize those different types explicitly. In particular, the failure probability due to a particular "cause", or, more properly, causal mechanism, is not estimated. The effect of the different causes is, instead, implicit in the parameter values of the CCF models. One of the main areas of concern in this approach is the difficulty of identifying the root causes, and assessing the strength of coupling and the quality of defenses, from the event reports which constitute the data base. The approach would benefit from a set of guidelines to assist an analyst in making these assessments, albeit from a somewhat imperfect and incomplete data set.

An application of Dorre's proposed procedure, by contrast, would employ an explicit representation of different behavior types, corresponding to different environments. A major challenge will be to define environments such that the conditional independence assumption holds. In addition, as pointed out also by Dorre, care must be taken to distinguish between two types of dependency, as discussed below.

DISTINGUISHING BETWEEN CAUSAL AND STATE OF KNOWLEDGE DEPENDENCY

In the currently adopted PRA methodology, it is important to distinguish between stochastic variability and uncertainty. Since the mathematics for dealing with both is the same, it is relative easy to confuse the two concepts and treat them as equivalent.

As an example, consider a model discussed in a paper by Lindley and Singpurwalla (1986) which in its mathematical structure resembles the model of Dorre. The idea behind the model is that the change from the test to the

actual environment modifies the behavior of components, and that this modification introduces a dependence between supposedly independent failures. They introduce a probability distribution on an environmental factor that characterizes the effect of the change. However, what this distribution represents is the uncertainty on the value of the factor, but is not intended to describe a stochastic variability. The dependence thus introduced is related to the state of knowledge dependence (Apostolakis and Moieni 1984), and has little to do with common-cause failures.

Mr. Dorre's model, in an apparently similar way, expands the probability of failure of a component as a weighted sum of a spectrum of failure probabilities thus representing explicitly the presence of different failure behavior characteristics in the space of possible failures. The different behaviors are characteristic of different "environments" and the weights represent a sampling distribution of the specific "environment" of a component. In his paper he states that the definition and characterization of an environment is a function of "engineering details, history and root causes of failure." In defining the environments, it is important to distinguish between factors that represent uncertainty about the base case, and factors that represent physical variability in the system of interest. As an example of the first kind of factor, in assessing the reliability of a new design without knowing the specific component type that will be used, and therefore its specific failure behavior, the probability distribution of environments might reflect an uncertainty on the appropriate base case component behavior to use, but not a stochastic process. The point is that the component at a particular plant when built, will have a particular initial failure behavior type, we just don't know which one it is. Our information base is the range and frequency of behaviors in a larger population of like component types, which can be used to characterize our uncertainty about one particular component, in much the same way that plant-to-plant variation of component failure rates has been used as a prior distribution in Bayesian analysis of plant-specific data. The manufacturer of a pump at an operating plant would not normally be identified as a stochastic variable.

An example of the second kind of factor is a factor that specifies the conditions affecting the component when a demand (randomly distributed in time) is made on it. These conditions represent the effect of stochastic factors, such as the occurrences of random external shocks on an operating plant, or the effects of aging, as distinct "environments". It is this type of factor that gives rise to the apparent dependency between basic events and is appropriate to the common-cause problem.

CONCLUSION AND SUMMARY

We have discussed why the common-cause failure concept, or some alternative, is necessary. While the common-cause failure models in themselves provide little insight into the vulnerabilities of systems, the process of trying to understand mechanisms of failure, and the ways that various factors influence the likelihood of multiple failures, does. However, it is clear that this process is as yet somewhat undisciplined. Hence papers such as these by Dorre, and the research being pursued by NRC (Parry et al, 1989) which are attempting to put some structure into the analysis of failure mechanisms are to be welcomed. From the point of view of quantifying system unavailability, however, the current common-cause models would appear to be adequate, given that a formal, defendable approach to estimating their parameters can be established. In particular, the use of failure modes, or failure mode and impact basic events, is a practical solution to the problem of reliability estimation.

REFERENCES

1. Apostolakis, G. and Moieni, P. (1987), "The Foundations of Models of Dependence in Probabilistic Safety Assessment", Reliability Engineering, Vol 18, pp. 177-195.

2. Dorre, P. (1989), "Basic Aspects of Stochastic Reliability Analysis for Redundancy Systems," Reliability Engineering and System Safety (to be published).

3. Lindley, D.V. and Singpurwalla, N.D. (1986), "Multivariable Distributions for the Life Length of Components of a System Sharing a Common Environment", Journal of Applied Probability, Vol. 23, No. 2, pp. 418-431.

4. Mosleh, A, Fleming, K.N., Parry, G.W., Paula, H.F., Worledge, D.H., and Rasmuson, D.M. (1988 Vol 1, 1989 Vol 2, "Procedures for Treating Common-Cause Failures in Safety and Reliability Studies, NUREG/CR-4780/EPRI NP 5013.

5. Parry, G.W., Paula, H.F., Mitchell, D.B., Whitehead, D.W., and Rasmuson, D.M. (1989), "A Cause-Coupling Defense Approach to Common-Cause Failure, presented at PSA '89, Pittsburgh, PA., April 3-7.