IAEA-TECDOC-648

Procedures for conducting common cause failure analysis in probabilistic safety assessment

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

The IAEA does not normally maintain stocks of reports in this series. However, microfiche copies of these reports can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 100,– in the form of a cheque or in the form of IAEA microfiche service coupons which may be ordered separately from the INIS Clearinghouse.

PROCEDURES FOR CONDUCTING COMMON CAUSE FAILURE ANALYSIS
IN PROBABILISTIC SAFETY ASSESSMENT
IAEA, VIENNA, 1992
IAEA-TECDOC-648
ISSN 1011–4289

Printed by the IAEA in Austria
May 1992

PLEASE BE AWARE THAT
ALL OF THE MISSING PAGES IN THIS DOCUMENT
WERE ORIGINALLY BLANK

FOREWORD

Probabilistic safety assessment (PSA) is increasingly important in the safe design and operation of nuclear power plants throughout the world. The Agency supports this trend and has focused on promoting, assisting and facilitating the use of PSA, by reviewing the techniques developed in Member States, assisting in the formulation of guidelines and helping Member States to apply such guidelines in order to enhance the safety of nuclear power plants.

In this context, a set of publications is being prepared to promote transfer of state of the art approaches to PSA modelling topics and to encourage consistency in the way PSA is carried out.

The publications, of which the present report forms a part, cover the role of PSA and probabilistic safety criteria in nuclear safety, provide guidance on the conduct of PSA and on specific topics such as external hazards, human reliability analysis, common cause failure analysis and computer codes for PSA.

EDITORIAL NOTE

In preparing this material for the press, staff of the International Atomic Energy Agency have mounted and paginated the original manuscripts and given some attention to presentation.

The views expressed do not necessarily reflect those of the governments of the Member States or organizations under whose auspices the manuscripts were produced.

The use in this book of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of specific companies or of their products or brand names does not imply any endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Throughout the world, countries with operating nuclear plants are recognizing the need for a quantitative expression of the safety of their plants. In some cases the need is to ensure that all plants conform to some prescribed safety level, expressed in terms of probability of core damage or release of radioactivity. In other cases the need is to verify whether design backfits or change in operational practices are needed and to choose between alternatives. A particularly recent development is the need to ensure that operating utility companies are prepared to deal with a severe accident and have thought through the required responses in some detail. Probabilistic Safety Assessment (PSA) is now a widely used tool for such beyond design basis analysis.

Most of the recently completed PSAs have found that common cause failures (CCFs) are significant contributors to core damage frequency. The analysis of common cause failures has undergone significant improvement over the last few years which has led to the writing of this document.

1.2. OBJECTIVE

The principal objective of this report is to supplement the procedure developed in Mosleh et al. (1988, 1989) by providing more explicit guidance for a practical approach to CCF analysis. The detailed CCF analysis following that procedure would be very labour intensive and time consuming. This document identifies a number of options for performing the more labour intensive parts of the analysis in an attempt to achieve a balance between the need for detail, the purpose of the analysis and the resources available.

The document is intended to be compatible with the Agency's Procedures for Conducting Probabilistic Safety Assessments for Nuclear Power Plants (IAEA, 1992), but can be regarded as a stand-alone report to be used in conjunction with NUREG/CR-4780 (Mosleh et al., 1988, 1989) to provide additional detail, and discussion of key technical issues.

1.3. STRUCTURE

In section 2 common cause failures are defined and an overview of the analysis procedure is presented. Section 3 discusses the definition of the scope of the analysis. Section 4 presents recommendations for CCF models and gives some guidance on data analysis and parameter estimation. The analysis of results is discussed in section 5, and some specific concerns in CCF modelling are addressed in section 6.

2. FRAMEWORK FOR COMMON CAUSE FAILURE ANALYSIS

This section provides the definition of common cause failure (CCF) events and an overview of the procedural framework. The description given here is only a brief summary of the detailed framework provided in the Procedures for Treating Common Cause Failures in Safety and Reliability Studies (Mosleh et al., 1988, 1989), which has also been adopted in the Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (IAEA, 1992).

2.1. DEFINITION

Common cause failure events are defined as multiple failures of components from shared root causes. From a practical point of view, the common cause failure events included in plant logic models represent those intercomponent dependencies which are considered to be potentially significant, and whose mechanisms are not explicitly represented in the logic model (event trees and fault trees) of the plant. It is important to emphasize that it is advisable to explicitly model specific dependent failure mechanisms whenever possible and to make a clear distinction between the coverage of such modelling on the one hand, and the scope of the common cause failure analysis on the other hand. This aspect will be further elaborated in section 3 dealing with the scope of common cause failure analysis.

2.2. OVERVIEW OF ANALYSIS FRAMEWORK

Four major stages, each of which contains a number of steps, form the procedural framework for the analysis. Figure 1 summarizes the main elements of the framework. Some comments are given below including the references to the sections of the present guidelines, which specifically cover the underlying concepts. For more detailed definitions we refer to the original reference (Mosleh et al., 1988, 1989).

Stage 1 - System Logic Model Development - is covered in the general guidelines for PSA (IAEA, 1992). This stage is a prerequisite for common cause failure analysis. Aspects related to the interface between that stage and the subsequent ones will be touched upon in section 3.

Stage 2 - Identification of Common Cause Component Groups - focuses on the screening process and is critical for definition of the scope of the detailed analysis. Due to its importance with respect to the choice of a suitable degree of detail, the characteristics of the screening procedures will be further described in section 3.

Stage 3 - Common Cause Modelling and Data Analysis - A definition of common cause basic events has been given in section 2.1. The incorporation of common cause events in the logic model is achieved by a straightforward modification of its structure. The selection of models for quantification of CCF contributions and the analysis and manipulation of data constitute the tasks which call for most guidance. Section 4 deals with these aspects.

Stage 4 - System Quantification and Interpretation of Results - synthesizes the key output of the previous stages leading to quantification of system failure probability. In addition, uncertainty and sensitivity analyses provide additional perspective for interpretation of results. This is discussed in section 5.

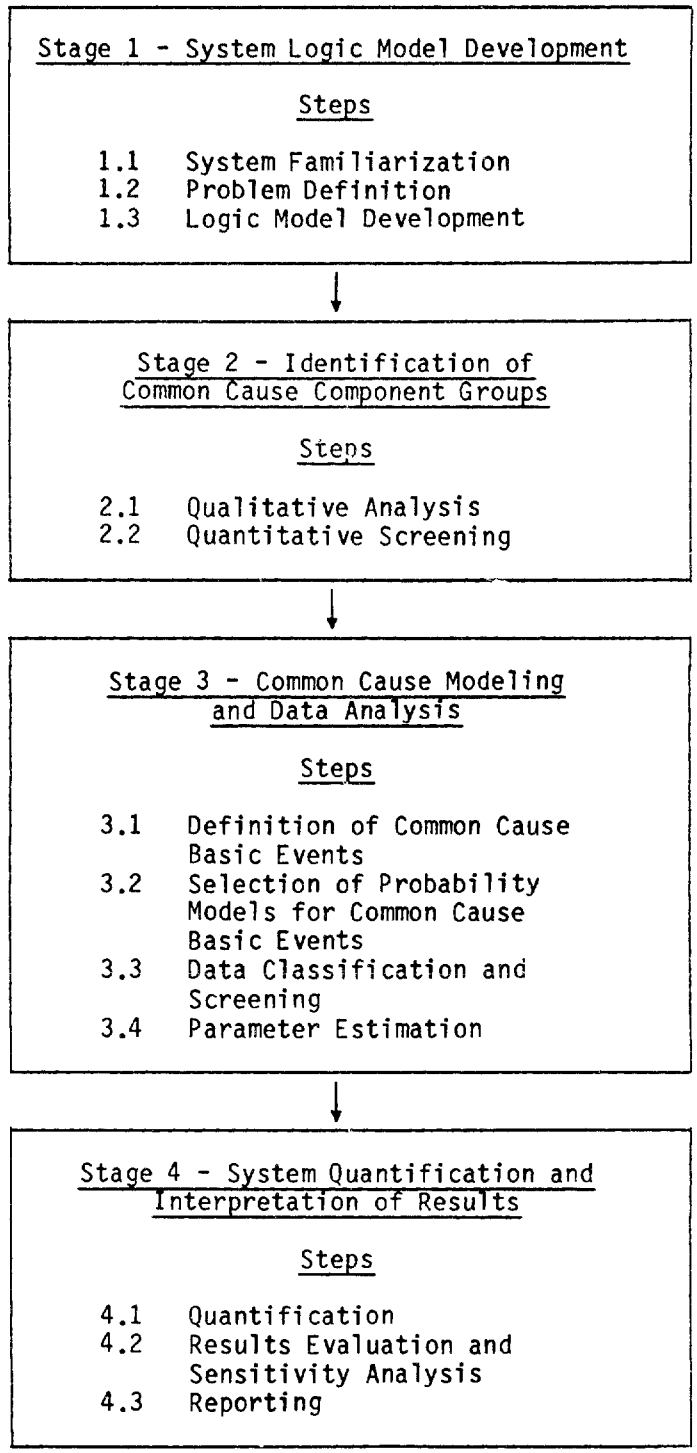

FIG. 1. Procedural framework for common cause failure analysis (Mosleh et al., 1988, 1989).

3. SCOPE OF COMMON CAUSE FAILURE ANALYSIS

As indicated in the objectives of the present guidelines (section 1.2), common cause failure analysis may represent a substantial effort which requires significant resources. Due to the potential importance of CCFs it is recommended that comprehensive qualitative and quantitative CCF analyses should be an integral part of each PSA. However, it is acknowledged that the scope of the studies must be in

balance with the available resources and might be affected by the particular objectives of a PSA. In addition, the degree of detail that can be reasonably expected and the choice of a suitable approach depend on a variety of analysis boundary conditions, e.g. collection of plant specific CCF data, on the database used for assignment of single failure probabilities, on the available evidence of CCFs experienced at the particular plant, on the relevance and transferability of external (generic or plant specific) data sources, and on the characteristics of the overall approach to the logical model of the plant.

Due to the reasons given above, the guidelines provided in this report offer different options with respect to the degree of detail in the context of common cause failure analysis.

The present guidelines are based on the analysis framework developed in the USNRC/EPRI procedures for treatment of CCFs (Mosleh et al., 1988, 1989), briefly summarized in section 2 of this report. It is assumed that the first stage of the framework, i.e. system logic model development, is carried out in accordance with the general PSA procedures prepared by the IAEA (IAEA, 1992). Consequently, it is important that categories of dependencies, such as functional (including shared equipment), physical and human interactions, and Common Cause Initiators (CCIs) are modelled explicitly to the extent that is practical in view of the information available. In addition, certain mechanisms for intercomponent dependent failures may be felt to be sufficiently important to be included explicitly in the model. For example, in the PSA performed for the Surry nuclear plant as part of the NUREG 1150 project (Bertucio et al., 1987), a mechanism for steam binding of the three trains (two motor driven, one turbine driven) of the auxiliary feedwater system was identified, and a term included in the fault tree model to represent this mechanism. The analysts responsible for integration of CCF contributions in the overall logic model must be aware of the extent of the explicit representation of such dependencies in order to avoid possible omissions and/or double counting. Another important aspect in this context is a clear specification of component boundaries to assure a proper distinction between the contributions covered by component failure data, and those corresponding to support functions, which are represented separately in the plant model. This issue is of central importance for the assessment of both single failure and CCF probabilities. Examples of thoroughly specified component boundaries may be found in the Swedish Reliability Data Book (Bento et al., 1985).

In the following, the discussion on the scope of common cause failure analysis will focus on stage 2 of the general framework, i.e. identification of common cause component groups. The objectives of this stage include (Mosleh et al., 1988, 1989):

- Identifying the groups of system components to be included in, or eliminated from, the CCF analysis;
- Prioritizing the groups of system components identified for further analysis so that time and resources can be best allocated during the CCF analysis;
- Providing engineering arguments to aid in data analysis (stage 3);
- Providing engineering arguments to formulate defence alternatives and stipulate recommendations in stage 4 (interpretation of results) of the CCF analysis.

The screening process serves as a tool for identification of groups of components which may be susceptible to common cause failure and helps to limit the scope of the analysis. Screening can be performed qualitatively and/or quantitatively.

Qualitative screening is considered as most important for the purpose of gaining engineering insights in the form of identification of possible plant specific weaknesses, which might eventually lead to a formulation of defensive strategies. Qualitative screening includes identification of root causes and coupling mechanisms for specific component groups, as well as consideration of existing defensive measures. A plant specific survey of all these factors is not only helpful as a basis for the screening process, it also serves as a good background for qualitative understanding of past events when carrying out the application-oriented screening in order to generate pseudo plant specific data. This aspect will be highlighted in more detail in section 4 of the present report.

The qualitative screening includes identification of attributes such as design, location, modes of operation and operational history etc. for various components in order to identify factors that might determine component interdependence. Examples of such factors are: similarity in component type and design characteristics, manufacturer, internal and external environments, location, testing and maintenance procedures, etc.

The generic cause approach (Rasmuson et al., 1982) offers a systematic and structured way to screen groups of components susceptible to common cause failures. In principle any combination of components could be postulated to have a potential for being involved in a common cause failure event. It is, therefore, recognized that extensive application of generic cause approach or other types of qualitative screening is time consuming.

However, there exist hardly any examples of full-scope PSAs where an in-depth qualitative screening has been applied to a large number of component groups. It is recommended that the scope of such an in-depth analysis be determined by application of quantitative screening, and by a priori selection of the types of components which in view of past experience should be the subject of more detailed analysis.

The present guidelines recommend that some component types, which, according to previous experience, are either particularly susceptible to common cause failures and/or are critical for the level of plant safety, should always be a subject of relatively detailed common cause failure analysis. The focus in this context is on active redundant components and intrasystem contributions. The comparative review of dependent failure analysis in six Swedish PSAs (Hirschberg, 1990) has shown that the principal CCF contributors are motor-operated valves and pumps. Other important CCF contributors might be diesel generators, batteries, gas turbines (if available), pressure relief valves, air-operated valves, check valves, scram valves, RPS-logic channels, breakers and sensors.

The results of PSAs performed in the USA generally support these conclusions, although CCFs of diesel generators and batteries have somewhat higher importance than in the Swedish plants. In addition, common cause failures of reactor scram breakers (PWR) have been considered important.

It is recommended that the above mentioned component types be considered in the CCF analysis as a minimum. The degree to which these CCF contributions and those for other identical, functionally non-diverse, active, redundant components should be investigated in detail may be determined by means of quantitative screening.

Quantitative screening includes implementation of common cause failure events for each component in a common cause failure group, assignment of screening numerical values to each contribution (e.g. by use of a presumably conservative beta factor of 0.1) and solution of the fault trees. The results of quantification may serve as a basis for final decisions with respect to:

- the need of detailed qualitative analyses for the minimal group of CCF contributors and for other candidates, as well as the need of detailed data analysis; and

- the need of representation of all applicable failure multiplicities.

The decision as to whether to perform a detailed analysis must be based on screening criteria. This must be established by the user once the preliminary results of the PSA, using these screening values, have been obtained. Clearly, if a particular CCF contributor is in one of the highest probability cut sets, it is a candidate for detailed analysis. If, however, the probabilities are essentially of the same order of magnitude for all the cut sets, then the highest probability cut sets may not have a dominant effect on total unavailability. Thus the decision to perform detailed analysis on any contributor is a function of its importance to the overall result. It must also be remembered that other parts of the analysis may be undergoing refinement at the same time (for example, the estimation of human error probabilities). Consequently, it is important to have a global perspective of the results in order to make effective use of resources for detailed analysis.

As a rule, fully diverse components are considered as not susceptible to CCF events. However, care must be taken with diverse components with identical piece parts. Clear specifications of component boundaries, mentioned earlier, will help to identify such situations. Also passive components are seldom subject to common cause failure analysis. However, checks should be made that events such as, for example, blockage of redundant pump strainers, have been explicitly represented in the logic model of the plant.

Another issue which influences the scope of analysis is the question of representation of all applicable failure multiplicities (e.g. inclusion of double, triple and quadruple CCFs in a plant designed with four redundant trains in safety systems). Neglect of lower failure multiplicities results in underestimation of the frequencies of accident sequences. In most cases the contributions of the lower failure multiplicities to the core damage frequency are low (Hirschberg et al., 1989), but the actual significance depends, for example, on the prevailing success criteria. Consequently, it is recommended that whenever possible all applicable failure multiplicities should be taken into account. In case simplified parametric models which only account for the highest failure multiplicity are used, checks should be made to verify that this approximation is reasonable. This is discussed further in section 6.

The scope of data analysis may vary as described in more detail in section 4. The preferred approach includes a thorough plant specific analysis. It is, however, recognized that parameter estimation in some cases has to be based on generic sources. In such situations, the minimum requirement would be to discuss the relevance of such sources and their applicability to the plant being analyzed.

Finally, given that a model and data have been selected and the analysis has been carried out, the results obtained should be subject to sensitivity and uncertainty analysis. Sensitivity analysis in particular is a primary tool to demonstrate the impact of modelling assumptions in common cause failure analysis on PSA results and conclusions. Section 5 will address this issue.

4. MODELS, PARAMETER ESTIMATION AND DATA ANALYSIS

4.1. INTRODUCTION

Many models have been proposed for the evaluation of common cause failures, but only those that have been used in performing PSAs belong to the classes referred to as parametric models or shock models. The European CCF benchmark exercise (Poucet et al., 1987) and the Scandinavian benchmark exercise (Hirschberg, 1987) both showed that the choice of CCF model is not important if a consistent set of data is used. Some of the available models have, however, a structure that can complicate data analysis. Other models, for example Dörre (1989) and Hughes (1987), have not been used in published PSAs. Consequently, only two models are discussed here, the Basic Parameter Model (Fleming and Mosleh, 1985), which is the most general form of the commonly used parametric models, and a particular reparameterization of that model called the alpha factor model (Mosleh and Siu, 1987). The estimation of the parameters of these models is discussed, pointing out different options available depending on the resources. Because of the importance of the qualitative aspects of historical event analysis, additional guidance is given over and above that given in Mosleh et al. (1988, 1989).

4.2. RECOMMENDED PARAMETRIC CCF MODELS

4.2.1. Basic Parameter Model

The most general of the commonly used parametric CCF models is the Basic Parameter Model. All the other parametric models can be characterized as reparameterizations of this model. In this model, a set of parameters $Q_k^{(m)}$ is defined as follows:

$Q_k^{(m)}$ = probability of a basic event involving k specific components ($1 \leq k \leq m$) in a common cause component group of size m

The model is based on a symmetry assumption that the probabilities of similar basic events involving similar types of components are the same. For example, if A, B and C comprise a common cause component group, then

$$P(A_1) = P(B_1) = P(C_1) = Q_1^{(3)}$$

$$P(C_{AB}) = P(C_{AC}) = P(C_{BC}) = Q_2^{(3)}$$

$$P(C_{ABC}) = Q_3^{(3)}$$

Note that, with the symmetry assumption, the probability of failure of any given basic event involving similar components depends only on the number and not on the specific components in that basic event.

Depending on the system modelling requirements, $Q_k^{(m)}$s can be defined as demand-based (frequency of failures per demand) or time based (rate of failures per unit time). The latter can be defined both for the standby failure rates as well as for the rate of failures during operation.

In terms of the basic specific parameters defined above, the total failure probability, Q_t, of a component in a common cause group of m components is

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k^{(m)}$$

where the binomial term

$$\binom{m-1}{k-1} = \frac{(m-1)!}{(m-k)!\,(k-1)!}$$

represents the number of different ways that a specified component can fail with (k-1) other components in a group of m similar components.

Assuming that the $Q_k^{(m)}$s are to be defined as demand based, it is shown in Mosleh et al., (1988, 1989) that the maximum likelihood estimators for $Q_k^{(m)}$ are given by

$$Q_k^{(m)} = \frac{n_k}{N_k}$$

where

n_k = number of events involving k components in a failed state

and

N_k = number of demands on any k component in the common cause group.

Thus in principle, to estimate the $Q_k^{(m)}$, one needs to count the number of events n_k, with k failures, and the number of demands N_k on all groups of k

components. The number of demands, N_k, is often estimated on the basis of the operating practices at the plant. For example, if, each time the system is operated, all of the m components in the group are demanded, and this number of demands is N_D, then

$$N_k = \binom{m}{k} N_D$$

The binomial term $\binom{m}{k}$ represents the number of groups of k components that can be formed from m components. We, therefore, have

$$Q_k^{(m)} = \frac{n_k}{\binom{m}{k} \cdot N_D}$$

The intermediate step of estimating the (N_k) can be avoided if, instead of using the basic parameter model, a reparameterization of that model is used, as described in section 4.2.2. This avoidance of direct estimations of the N_k is useful when a well-established data base exists for the single failure event probabilities that is different from the data base that will be used for the common cause failure analysis. This happens when, for example, plant specific data is sufficient to produce reliable estimates for individual component failure rates or probabilities, but not for common cause failure rates or probabilities. This is the most common situation. There are many possible parametric models, but for the reasons explained in Mosleh and Siu (1987) the preferred model is the alpha factor model.

4.2.2. **The Alpha Factor Model**

The alpha factor model defines common cause failure probabilities from a set of failure frequency ratios and the total component failure probability Q_t. In terms of the basic event probabilities, the alpha factor parameters are defined as

$$\alpha_k^{(m)} = \frac{\binom{m}{k} Q_k^{(m)}}{\sum_{k=1}^{m} \binom{m}{k} Q_k^{(m)}}$$

where $\binom{m}{k}$ $Q_k^{(m)}$ is the probability of events involving k component failures in a common cause group of m components, and the denominator is the sum of such probabilities. In other words,

$\alpha_k^{(m)}$ = *ratio of the probability of failure events involving any k components* over the total probability of all failure events in a group of m components.

For example, for a group of three similar components we have

$$\alpha_1^{(3)} = \frac{3Q_1^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}}$$

$$\alpha_2^{(3)} = \frac{3Q_2^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}}$$

$$\alpha_3^{(3)} = \frac{Q_3^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}}$$

and $\alpha_1^{(3)} + \alpha_2^{(3)} + \alpha_3^{(3)} = 1$ as expected.

We can see that the basic event probabilities can be written as a function of Q_t and the alpha factors as follows:

$$Q_k^{(m)} = \frac{m\alpha_k^{(m)}}{\binom{m}{k}\alpha_t} Q_t$$

where

$$\alpha_t = \sum_{k=1}^{m} k\,\alpha_k^{(m)}$$

An estimator for each of the α factor parameters (α_k) can be based on its definition as the fraction of total failure events that involve k component failures due to common cause. Therefore, for a system of m redundant components,

$$\alpha_k = \frac{n_k}{\sum_{k=1}^{m} n_k}$$

Thus, in this case, to evaluate the CCF contributions, it is only necessary to estimate Q_t, and measure the various n_k, but estimates of the N_k are not directly required. However, it should be noted that the assumptions that go into estimating N_k are embedded in the formulation of the α factor model. This is discussed in Appendix C of Mosleh et al. (1988, 1989).

Thus, in order to estimate CCF contributions, it is necessary to obtain N_D, n_1, ..., n_m for the basic parameter model, or to already have an estimate of Q_t, and obtain n_1, ..., n_m for the α factor model.

4.3. PARAMETER ESTIMATES AND DATA ANALYSIS

4.3.1. **Plant Specific Estimates**

It is generally considered that CCFs are plant specific. Thus the most appropriate estimates of CCF model parameters would be obtained from plant specific data. However, nuclear power plant components are generally very reliable, and only few significant independent failures are expected for any population of components. Multiple failure events are even rarer and a statistically adequate, plant specific, data base for evaluating CCF probabilities is highly unlikely to be available. It is because of this that the procedure for pooling data from a variety of plants, and trying to construct a pseudo plant specific data base by reinterpreting historical events in the context of the plant in question, was developed (Mosleh et al., 1988, 1989).

4.3.2. **Construction of Pseudo Plant Specific Data Base and Parameter Estimates**

Application of the data analysis process is very time-consuming and, furthermore, in Mosleh et al. (1988, 1989), there is little guidance on how this should be performed. However, it is an important step in order to gain insight into the potential ways that CCFs can occur, and it is as much for this, as for improving the parameter estimates themselves, that the following process is recommended. In this subsection some ideas are introduced to help analyzing the data.

4.3.2.1. Guidelines for Historical Event Interpretation

In principle, each event associated with inoperability of equipment should be identifiable with a basic event of the model. There are two basic features of the event description which are necessary to make this identification.

The first is the effect of the event, which guides the analyst to a particular basic event of the model or a particular gate, e.g. RHR pump A inoperable - unable to perform its function. The second basic feature describes the cause, which, together with a knowledge of the boundaries of the basic events of the models, enables the correct allocation to be made; for example, if the cause is de-energization of the 4.16 KV bus, then the event is associated with the bus unavailability, not the pump. If it is a local fault of the pump or its breaker, it is associated with the pump component itself. For standby components, such as pumps, it is necessary to distinguish between failure to start and failure to run - this is not always straightforward.

The following are some ground rules for event allocation.

1. If the cause of unavailability of a standby component is self-revealing at the time it occurs, or occurs during a test but is revealed at the end of a test, and results in maintenance, the event is accounted for in the unavailability due to maintenance. The event may also be counted towards estimation of the failure to perform the mission.

2. Failures to start or run are characterized by the failure condition not being revealed before a test or an actual demand and the failure being catastrophic

(in the sense of preventing operation, or preventing operation above a certain minimum performance level).

3. Failures, such as leaks of components (i.e. pumps and valves), which are not serious enough to be failures of the pressure boundary by an accepted definition, would be included in the unavailability due to maintenance, as their effect is to induce maintenance activity.

4. If the effect, for example pump A fails, is the result of the failure of another component that is modelled explicitly, the event is associated with that component, not the pump.

5. If the failure is caused by the test itself, or can only occur under test conditions, it should not be considered if the test conditions are beyond those normally expected on a real demand.

6. If the failure is spurious and could not be repeated on an immediate second test or subsequent tests, it could be included as a potential failure but to a best estimate it is not a failure. In the same way, events which are instantly recoverable are not important failures. This is of course a function of the success criterion for the component in terms of the time window within which it has to be operating.

7. Failures caused by the tests performed as part of troubleshooting are not valid failures.

8. An event only reporting a degraded component state, e.g. failure of one air start motor of a diesel generator which has redundant air start motors, should be carefully excluded from the failure events.

Given that the above guidelines help identify failure events, it is important also to consider how to identify common cause failure events. The following guidelines are suggested:

1. If possible, a single causal root mechanism should be identified as the cause of the multiple failure event.

2. The time period within which the failures can occur is an important concern. For standby components, the failures must occur within the minimum time between effective opportunities to reveal the faults. For operating components they must occur within the mission time used for the PSA. Since the mission time is generally considerably longer than the operating test time for standby components such as pumps, special consideration has to be given to events that include degraded states of components. A judgement should be made as to whether the degradation is such that it might have led to failure within the mission time.

3. Cascade failures and other dependencies which originate from basic design principles (e.g. functional dependencies related to power supply, signal exchange or to other explicitly modelled auxiliary systems), are not regarded as CCFs.

4. Many failures are not manifested as multiple, since measures are taken to prevent them before they occur. In some cases the failure event has such a character that even if only a single failure has actually occurred, the onset of the same failure mechanism with the same cause may be detected in other units. Furthermore, seemingly independent multiple failures which occur close in time cannot a priori be regarded as fully independent. Such failures should be identified as potential CCFs. This category can even include components in degraded condition whenever they occur in conjunction with actual failures in a dependent fashion, as discussed under 2.

5. The aim of the analysis is to identify all relevant CCF events which involve identical components within each plant. Consequently, the analysis need not, a priori, be limited to redundant components within a single system. It is, however, expected that the evidence of CCFs involving identical components within different systems (intercomponent - intersystem CCFs) will be rather weak. Also, most PSAs to date have not included intersystem CCFs.

Given a set of failure events, both single and multiple, the CCF procedure requires them to be interpreted for their CCF potential.

Mosleh et al. (1988, 1989), section 5, proposed discussing CCFs using the concepts of root causes, coupling mechanisms and defensive mechanisms. This suggests a causal picture of failure with the identification of a root cause, a means by which the root cause is more inclined to impact on a number of components simultaneously (the coupling), and the failure of the defences against such multiple failures. This concept has been developed to some degree as a means of providing guidance for event interpretation (Paula and Parry, 1990).

Failure Causes

It is recognised that the description of a failure in terms of a single "cause" is often too simplistic. For example, for some purposes it may be quite adequate to identify that a pump failed because of high humidity. But to understand, in a detailed way, the potential for multiple failures, it is necessary to identify further why the humidity was high and why it affected the pump (i.e., it is necessary to identify the ultimate cause of failure). There are many different paths by which this ultimate cause for failure could be found. And the sequence of events that constitute a particular failure path, or failure mechanism, is not necessarily simple. As an aid to understanding failure mechanisms, the following concepts are proposed:

A proximate cause that is associated with a failure event is a characterization of the condition that is readily identifiable as leading to the failure. In the above example, humidity could be identified as the proximate cause. The proximate cause in a sense can be regarded as a symptom of the failure cause, and it does not in itself necessarily provide a full understanding of what led to that condition. As such, it may not, in general, be the most useful characterization of failure events for the purposes of identifying appropriate corrective actions.

To expand the description of the causal chain of events resulting in the failure, it is useful to introduce the concepts of conditioning events and trigger events. These concepts are introduced as an aid to a systematic review of event data and are

particularly useful in analyzing component failures from environmental causes. But it is not always necessary or convenient to consider both concepts.

A conditioning event is an event which predisposes a component to failure, or increases its susceptibility to failure, but does not of itself cause failure. In the previous example (pump failed because of high humidity), the conditioning event could have been failure of maintenance personnel to properly seal the pump control cabinet following maintenance. The effect of the conditioning event is latent, but the conditioning event is in this, and in many other cases, a necessary contribution to the failure mechanism. A trigger event is an event which activates a failure, or initiates the transition to the failed state, whether or not the failure is revealed at the time the trigger event occurs. An event which led to high humidity in a room (and subsequent equipment failure) would be such a trigger event. A trigger event therefore is a dynamic feature of the failure mechanism. A trigger event, particularly in the case of CCF events, is usually an event external to the components in question.

It is not always necessary, or even possible, to uniquely define a conditioning event and a trigger event for every type of failure. However, the concepts are useful in that they focus on the ideas of an immediate cause, and subsidiary causes, whose function is to increase susceptibility to failure, given the appropriate ensuing conditions. Some examples of the use of these concepts are given in Table I.

The next concept of interest is that of the "root cause". The root cause, following Gano (1987), is the basic reason or reasons why the component(s) fail, any of which, if corrected, would prevent recurrence. The identification of a root cause, therefore, can be seen to be tied to the implementation of defences.

As shown in Table I, the root cause may be a trigger event (second event in the table) or a conditioning event (third event). It is clear from Events 1 and 4 in Table I that many proximate causes (moisture and vibration) are indeed only symptoms of the root cause, and that the proximate causes do not in themselves provide a full understanding of what led to that condition. All too often, investigations of failure occurrences (and thus the event descriptions in failure reports and in data bases) do not determine the root causes of failures, even though this determination is crucial for judging the adequacy of defences against these failures.

Coupling Factors and Mechanisms

For failures to become multiple failures from the same cause, the conditions have to be conducive for the trigger event and/or the conditioning events to affect all the components simultaneously. The meaning of simultaneity in this context is that failures occur close enough in time to lead to inability of redundant components to perform the mission required of the redundant system of which they are a part. It is convenient to define a set of coupling factors. A coupling factor is a characteristic of a group of components or piece parts that identifies them as susceptible to the same causal mechanisms of failure. Such factors include similarity in design, location, environment, mission and operational, maintenance, and test procedures. These, in some references, have been referred to as examples of a coupling mechanism, but because they really identify a potential for common susceptibility, it is preferable to think of these factors as factors which help define a potential common cause component group.

TABLE I EXAMPLES THAT ILLUSTRATE CONCEPTS USEFUL IN ANALYZING CCFs (Paula and Parry, 1990)

	Failure Event	Proximate Cause	Trigger Event	Conditioning Event	Root Cause
1	A pump fails to run because of moisture in the pump control cabinet	Corrosion from moisture or high humidity	Event leading to the occurrence of high humidity (e.g., steam leak in pump room)	Failure to properly seal the control cabinet following maintenance	Lack of attention during maintenance ***and/or*** deficiency in the written procedures
2	A design error is such that under real demand conditions a component fails to perform its function (component had successfully performed its function during testing)	Design error	Design error	None	Error in design realization ***and*** failure to realize that proof testing was not adequately simulating real demand conditions
3a	Following a maintenance act, a component fails The failure is eventually attributed to an error in the maintenance procedure	Maintenance error	Maintenance act	Error or ambiguity in maintenance procedure	Error or ambiguity in maintenance procedure ***and*** inadequate training
3b	Following a maintenance act, a component fails The failure is eventually attributed to a slip on the part of the maintenance crew	Maintenance error	Maintenance act	Inadequate training and lack of attention during maintenance	Inadequate training ***and*** lack of motivation
4	A pump shaft fails because of the cumulative effect of high vibration, resulting from an installation error	Vibration	Cumulative exposure of the pump to the excessive vibration	Installation error	Inadequate training of installation crew ***and*** deficiency in installation procedures

In fact, it is questionable whether it is necessary to talk about a coupling mechanism as an entity separate from the failure mechanism. What is important is to identify the specific features of the coupling factors that lead to a simultaneous impact on the components in the group. This is a function of how the trigger and conditioning events are introduced at the system or common cause component group level. So, for example, in the four examples discussed in Table I:

1. More than one pump may fail if the conditions of high humidity exist in more than one control cabinet. However, for this to happen, all control cabinets have to be susceptible to moisture intrusion, and they also have to be located in a similar environment. Following from the previous example, if there were a conditioning event of failing to seal the cabinets properly, it would have to have occurred in more than one cabinet, and in addition, the trigger event causing the high humidity would have to affect the cabinets simultaneously (within our definition of simultaneity), for there to be a CCF. This implies a common domain of influence of the source of the trigger event and the conditioning event.

2. Components of the same design in a similar usage will all fail on a common demand if there is a fatal design error. The trigger event (the design error) is common to all components in the group, and is introduced simultaneously into the group.

3. There are many ways a maintenance related error can propagate to affect the system, depending on how it arose. For example, a basic error in the procedure would systematically affect all crews, no matter when they carry out maintenance. The conditioning event (i.e., the procedural error) is common to all crews. On the other hand, ambiguity in the procedure may result in one crew adopting an alternative approach consistently, no matter when they perform the maintenance. The ambiguity in the procedure represents a conditioning event; the trigger event is the particular maintenance activity in which the crew misinterprets and misapplies the procedures. In this case, the crew acts as the agent introducing the failure. However, the failure may still not become a CCF unless the crew performs the maintenance on redundant equipment close enough in time with respect to opportunities for discovery of the error (the frequency of maintenance is greater than the frequency of the appropriate tests).

   Slips or errors made during maintenance (Event 3b in Table I) are unlikely to be sources of CCFs unless maintenance is performed on several redundant components during a short time interval. If this were the case, it would be a coupling introduced by the specific way maintenance is performed.

4. A common, systematic, installation error could lead to simultaneous high levels of degradation. The coupling of failures is introduced into the system through a conditioning event, and is activated by the trigger event.

What is clear is that the way the potential for coupling is activated varies for the different conditioning and trigger events. In addition, it is clear that it is not easy to separate the concepts of the coupling and failure mechanism; coupling can occur at all points of the causal chain to some degree or other.

Defences

CCFs can be prevented by a variety of defences. A defence can operate to prevent the occurrence of failures. An example related to the first event in Table I would be to ensure that control cabinets are adequately protected against humidity by a quality control (QC) of the seals. This is equivalent to ensuring the hardening of the components, and is a defence against potential conditioning events. Another example of a defence that attempts to prevent the occurrence of failures is the training of maintenance staff to ensure correct interpretation of procedures. The coupling factors are not being directly affected by these two defences.

Another approach to defend against CCFs is to decouple failures (as opposed to prevent the occurrence of failures) by effectively decreasing the similarity of components and their environment in some way that prevents a particular type of failure cause from affecting all components simultaneously and allows more opportunity for detecting failures before they appear in all components of the group. For example, diversity in staff may prevent multiple failures that result from human-related maintenance errors. (Although it would not necessarily reduce the frequency of single failures from such errors.)

The key to successful mitigation and prevention of CCFs is to understand how the primary defences might fail. In the examples considered previously, the following are plausible reasons why the failures occurred, in terms of failure of defences.

1. If the error were that, at the design stage, it was not envisioned that a high humidity condition might arise, the design review process was potentially deficient. On the other hand, as assumed in Table I, the failure may have been a failure to maintain an adequate barrier against moisture intrusion, given that it was realized that such a barrier was necessary.

2. The design review process as a primary defence and proof testing as a secondary defence were deficient.

3. Insufficient or inadequate training could have led to the conditioning of a particular crew such that they had a high likelihood of making errors (Event 3b in Table I). In another case (Event 3a in Table I) it could have been a failure in the procedures review process that resulted in faulty or ambiguous procedures. In the case of ambiguous procedures, training can be a secondary defence. An error resulting from ambiguous procedures can therefore be regarded as resulting from a failure of two defences, the procedures review and training.

4. The QC process during installation was deficient, allowing an installation error to go undetected. The installation error in itself was the result of inadequate training of the installation crew and deficiencies in procedures.

For the purposes of discussion, a new set of general defensive tactics are defined below. They are to be regarded as general tactics implemented to decrease the likelihood of component or system unavailability. Many of the descriptions are adapted from Smith et al. (1988).

Barriers	Any physical impediment that tends to confine and/or restrict a potentially damaging condition.
Personnel Training	A programme to ensure that the operators and maintainers are familiar with procedures and are able to follow them during all conditions of operation.
Quality Control	A programme to ensure that the product is in conformance with the documented design, and that its operation and maintenance take place according to approved procedures, standards, and regulatory requirements.
Redundancy	Additional, identical, redundant components added to a system for the purpose of increasing the likelihood that the number of components required to perform a given function will survive exposure to a given cause of failure.
Preventive Maintenance	A programme of applicable and effective preventive maintenance tasks designed to prevent premature failure or degradation of components.
Monitoring, Surveillance Testing, and Inspection	Monitoring via alarms, frequent tests, and/or inspections so that failures from any detectable cause are not allowed to accumulate. This includes special tests performed on redundant components in response to observed failures.
Procedures Review	A review of operational, maintenance, and calibration/test procedures to eliminate incorrect or inappropriate actions that could result in component or system unavailability.
Diversity	The use of totally different approaches to achieve roughly the same results (functional diversity) or the use of different types of equipment (equipment diversity) to perform the same function. Equipment diversity can be considered in terms of construction, physical characteristics, applying this applying this concept. Diversity is a tactic that specifically addresses CCFs.

Cause-Defence Matrices

The analysis of the generic data can be used to construct cause defence matrices to record the insights gained. An example matrix is shown in Tables II and III, taken from Paula and Parry (1990). The construction of such matrices for all

TABLE II. ASSUMED IMPACT OF DEFENSES ON SELECTED FAILURE MECHANISMS FOR DIESEL GENERATORS (Paula and Parry, 1990)

	Selected Defenses Against Root Causes											
	General Administrative/Procedural Controls				Specific Maintenance/Operation Practices				Design Features			
Selected Failure Mechanisms for Diesel Generators	Configuration Control	Maintenance Procedures	Operating Procedures	Test Procedures	Governor Overhaul	Drain Water and Sediment from Fuel Tanks	Corrosion Inhibitor in Coolant	Service Water Chemistry Control	Air Dryers on Air Start Compressors	Dust Covers with Seals on Relay Cabinets	Fuel Tank Drains	Room Coolers
Corrosion products in air start system		o		o					■	-		
Dust on relay contacts		o		o						■		
Governor out of adjustment		o		o	■							
Water sediment in fuel		o		■		■					■	
Corrosion in jacket cooling system		o					■			-		
Improper lineup of cooling water valves	■	o		o								
Aquatic organisms in service water		■	■					■				
High room temperature		o										■
Improper lube oil pressure trip set point		o		o								
Air start system valved out	■	o		o								
Fuel supply valves left closed	■	o		o								
Fuel line blockage				o								
Air start receiver leakage									o			
Corrective maintenance on worn diesel generator	■	■										

TABLE III. ASSUMED IMPACT OF DEFENSES ON SELECTED COUPLING MECHANISMS FOR DIESEL GENERATORS
(Paula and Parry, 1990)

Selected Failure Mechanisms for Diesel Generators	Selected Defenses Against Coupling						
	Diversity			Barrier		Testing and Maintenance Policy	
	Functional	Equipment	Staff	Spatial Separation	Removal of Cross-ties (or Implementation of Administrative Controls)	Staggered Testing	Staggered Maintenance
Corrosion products in air start system	■	-	-	-	-	-	o
Dust on relay contacts	-	-	-	o	-	o	o
Governor out of adjustment	-	o	o	-	-	-	o
Water/sediment in fuel	■	-	-	-	o	-	-
Corrosion in jacket cooling system	■	-	-	-	-	-	-
Improper lineup of cooling water valves	■	-	■	o	-	■	■
Aquatic organisms in service water	■	-	-	o	o	-	o
High room temperature	-	-	-	o	-	-	-
Improper lube oil pressure trip setpoint	■	■	■	o	-	■	■
Air start system valved out	■	-	■	o	-	■	■
Fuel supply valves left closed	■	-	■	o	-	■	■
Fuel line blockage	■	-	■	-	-		-
Air start receiver leakage	■	-	-	-	■	-	-
Corrective maintenance on wrong diesel generator	■	o	■	o	-	o	-

components is very time consuming, but provides a systematic way of recording the insights and also a guide for future studies as to what features to look for in the defences at a plant to assess the potential for CCFs. The cause-defence information is qualitative: a solid square (▪) represents a strong defence, an open circle (o) represents a relatively weak defence, and a dash (-) represents no defence.

An example of practical implementation of the cause-defence matrices and of accounting for the influence of defences is presented in Himanen et al. (1989).

4.3.2.2. Event Reinterpretation

The process of event reinterpretation to construct the pseudo plant specific data base involves identifying whether the trigger and/or conditioning events that occurred at the initial plant could also occur at the target plant, and to try to assess whether the quality of the defences at the target plant are such that they would prevent the trigger and conditioning events from occurring simultaneously, or whether they would be more likely to result in multiple failures. This is clearly very subjective and dependent on the quality of the data base available. However, the process itself is worthwhile because of the increased understanding of CCF mechanisms it affords.

4.3.2.3. Choice of Data Base

In Mosleh et al. (1988, 1989) the recommended data base is the Nuclear Power Experience (NPE) (S. M. Stoller - continuously updated). However, this choice is largely based on US nuclear plant experience and may not be the most appropriate data source to use. In countries such as France and Sweden, which have their own data collection schemes, these data sources may be more appropriate. Nevertheless, the NPE data base is generally available, and may be the only source. In this case it has to be used carefully, recognizing that there may be internal inconsistencies, for example the component boundary definitions may be different at different plants. It does however provide a spectrum of failure mechanisms and significant qualitative insights, even if the quantitative estimates are subject to large uncertainty.

4.3.2.4. Parameter Estimation

Sections 3.3.3.3 through 3.3.3.5 in Mosleh et al. (1988, 1989) describe how event interpretation and reinterpretation can be summarized in terms of impact vectors. Section 3.3.3.4 in particular demonstrates how adjustments can be made to the impact vector to account for any difference in size between the CCF group in the initial plant, where the event occurred, and the target plant. This adjustment is made individually for each event. The summation over each of the components of the impact vector, provides the final pseudo plant specific data base in terms of the number n_k of events in which k components failed. These values are then used in the parameter estimators discussed in section 4.1. The results of a PSA may be sensitive to the particular features of the adjustment scheme chosen. Alternative schemes to that proposed in Mosleh et al. (1988, 1989) can be defined. A practical way of studying the uncertainties associated with this issue is to carry out sensitivity studies of the assumptions made in this context.

4.3.3. Generic Parameter Estimates

If the resources are not available to perform the more detailed CCF analysis discussed in section 4.3.2, or if indeed there is insufficient data, the only alternative is to use generic parameter estimates. This is not generally recommended as it does not provide any insight into what precautions could be taken, or defences implemented at the plant to improve safety. What it would provide is a means of incorporating, into the estimate of core damage frequency, a measure of some (ill-defined) industry average CCF potential.

There are various sources available, but one of the most useful is Fleming and Mosleh (1985). This document provides generic estimates, although these should be used with care, as they are averaged over failure mode. They are also based on a particular interpretation of historical events. However, the report does include brief descriptions of all the multiple failure events that went into making the estimates, and these are useful for a comparison with the target plant. It should be realized though that, because the single events are not described, reinterpreting the events as described above can only lead to a decrease of the common cause factors.

In many cases, it can be argued that, for those components for which little or no data is available, their failure probabilities or failure rates should be low and they are not likely to be significant contributors to core damage frequency, and a conservative generic beta factor of 0.1 is likely to be adequate. However, there may be cases where an engineering assessment is necessary to support lower numbers.

5. ANALYSIS OF RESULTS

The results of a common cause analysis may, at one extreme, be essentially quantitative, constituting estimates of common cause failure probabilities based on generic parameter estimates. At the other extreme, the quantitative analysis is supported by an in-depth qualitative analysis which provides the opportunity to identify potential weaknesses in the plant defences against the occurrence of multiple failures.

It has to be recognised that the estimation of the CCF model parameters has, associated with it, considerable uncertainty. The detailed analysis proposed in Mosleh et al. (1988, 1989) is dependent on a data base, which may have substantial deficiencies, and requires the analyst to make judgements as to the cause, applicability, and impact of the historical events. It is essential that the results of the PSA be qualified to recognize this uncertainty. A formal approach to qualifying the estimates of core damage frequency is to construct a distribution of the CCF failure probabilities, which covers all sources of uncertainty, but particularly that of interpreting the event reports and propagate that uncertainty through the analysis in the usual way. A general approach to doing this is outlined in section 3.3.4.4 of Mosleh et al. (1988, 1989). This is a very complex analysis if there are a large number of historical events to be analyzed. The propagation of uncertainty, performed in this way, would be useful for qualifying the analysts' confidence in the bottom-line result,

core damage frequency, but provides little information on the significance of the relative contributions, and, in practice such a detailed uncertainty analysis has not been performed. Some short cut methods were discussed in Mosleh et al. (1988, 1989). The significance of the contributions of basic events is generally assessed by using point estimates which are mean values of the probability distributions on these event probabilities. It is important to perform sensitivity analyses on the value of the CCF probabilities to have some feeling for the possible range of importance of their contribution.

It is generally agreed that common cause failure probabilities represent, at most, typically a factor of 0.2 of the single component failure probabilities and this, therefore, would be a reasonable worst case scenario. The best case scenario is that the common cause failure probabilities are zero. This sensitivity case would give a measure of the maximum possible improvement.

If the PSA is to be used to identify areas for plant improvement, then one has to rank the various CCF terms along with other candidates. It has to be remembered that the CCF failure probability may be anchored to a single component failure probability that has been obtained from a different source than the CCF model parameters. For example, using the alpha factor model, the Q_t may have been obtained from plant specific data, and the alpha factors from a generic data source such as NPE. Thus the CCF contribution may be reduced by decreasing Q_t as well as by decreasing the alpha factors.

Having established that there are some candidates for plant improvement, it has to be decided what improvement is possible or effective. The qualitative analyses performed in support of quantification will clearly be of help in this process.

However, it is somewhat limited in that it is based on the historical events only. Ideally, the lessons learnt from the review should be generalized to try to be more complete in assessing potential weaknesses in the plant defences, and hence potential fixes. Clearly, however, an analysis based on using generic parameter values will provide little input to this aspect of the analysis of the results.

6. PRACTICAL CONSIDERATIONS

6.1. INTRODUCTION

There are some practical concerns that arise when applying the methodology of Mosleh et al. (1988, 1989). There is a general concern about the modelling of high redundancy systems which is discussed in section 6.2. The discussion is split into two parts; the first concerns systems of high redundancy, the second systems of ultra high redundancy, with m, the degree of redundancy, in the order of 5 or higher. Another concern, associated with the identification of CCF component groups is discussed in section 6.3. While some of this material is contained in Mosleh et al. (1988, 1989), it is included here to give it greater prominence.

6.2. MODELLING OF HIGH REDUNDANCY SYSTEMS

6.2.1. **Cut Set Proliferation**

The first concern raised here is that of the proliferation of cut sets, and its impact on the solution of the system fault trees. Adoption of the alpha factor, or basic parameter model, implies that each basic event associated with a member of the CCF component group is effectively substituted by a number of basic events depending on the degree of redundancy. So, for a system of redundancy 3 (represented by A, B, C) each basic event for A, say, is substituted by

$$A_I + C_{AB} + C_{AC} + C_{ABC}$$

in the language of Mosleh et al. (1988, 1989). For a system of redundancy 4, each basic event is replaced by 8 basic events and so on.

This increases the size of the tree considerably and can lead to problems with its solution. There are at least two approaches to solving this problem. The first is to perform the model solution without inclusion of common cause failure terms, and then to perform cut set substitution and reminimalization. A major concern here is that the original solution should not be performed with a cut-off value that is too high, so that the components of interest could disappear from the model.

Another approach is to include only that term of the model which affects all the components or the maximum number k ($k<m$) required for failure by the system success criterion, that is to perform the substitution $Q_I + Q_m$ or $Q_I + \sum_{j=k}^{m} Q_j$ only. This should not be confused with the beta factor model, as the parameters are evaluated taking into account the events of different multiplicity as discussed in section 4. This approach is only valid if it can be assured that this global common cause term really does dominate. This may be difficult to establish a priori. For example, for a simple 1 out of 3 system with only one component per train, it requires demonstrating that

$$Q_3 >> 3\, Q_1\, Q_2$$

For more than one component per train the equation clearly becomes more complicated, requiring all combinations of component cut sets to be taken into account, as in the following equation

$$\sum_i 3\, Q_1^{(i)} \,.\, Q_2^{(j)}$$

which may be used to compare with $Q_3^{(j)}$. The superscript (i) runs over all components in the train model, and (j) indexes the CCF component group of interest.

Care has to be taken, however, that before performing such an a priori estimation the correct expression for the success criterion is used, and that the CCF

component group really does display the symmetry that is assumed. Some questions of symmetry are discussed in section 6.3.

Whichever of these approximations is made, it has to be performed with care as the above discussions show.

6.2.2. **Ultra High Redundancy Systems**

Some systems have a very large number of components for which common cause failure may be a concern. Cases of interest comprise e.g. pressure relief valves, control rods and fine motion drives, scram modules (Swedish reactors). A survey of Swedish PSAs has been made with the purpose of clarifying the approaches (i.e. assumptions, data, quantification methods) used. Incorrect extrapolations of simple parametric methods have been observed in several cases. Application of an extended Common Load (CL) model has been recently proposed as a solution to this problem (Mankamo and Kosonen, 1988).

The problems differ with changing success criteria. For example, the success criteria may be such that a large number of components must fail to cause loss of the function. This is true for the depressurization function in GE BWR. One problem is that no data exists for very large numbers of simultaneous failures, hence an approach based on the alpha factor or basic parameter models is faced with the problem of zero events for the parameters of interest. The parameter values have then to be based on engineering judgement. There seems to be little point in developing a model in this case that has any more than a total common cause failure term Q, and hence only the catastrophic, lethal common cause failure term is of interest. Estimating the probability of this term should involve a detailed understanding of the way the system is engineered and operated. An example is given in section 6.3.3.

On the other hand, the success criteria may be such that failure of a relatively small number of the components leads to loss of the function (e.g. control rod drive mechanisms in BWRs). In this case the assumption of a global common cause term may be substantially non-conservative due to the combinatorial factors associated with the lower order terms. A reasonable approach is to simplify the model to include CCF events which represent failures of 2, 3, 4 and all the components.

6.3. CCF COMPONENT GROUPS - BREAKING THE SYMMETRY

Three examples, taken from (unidentified) PSA studies and somewhat simplified are used to illustrate the importance of interfacing with the systems analysts and systems engineers to ensure an appropriate identification of CCF component groups, and inclusion of subgroups in the model to incorporate the effects of asymmetries.

6.3.1. **Example 1 - Functional Asymmetry**

The first example is that of a two unit BWR plant with four diesel generators, but only three emergency service water (ESW) pumps. Each diesel generator feeds a specific emergency bus, and the ESW pumps are fed from three specific buses. Under

normal circumstances, with complete symmetry, one would probably argue that, given that one diesel generator is adequate for both units, only the common cause failure of four diesel generators needs to be modelled. However, if only the three diesel generators associated with the ESW pumps fail, the emergency operating procedures direct the operators to connect the fourth diesel to one of the other buses, to assure a supply of cooling water for that diesel generator and the other cooling loads. Thus, if the model is to include this important operator action, it is necessary to model also the common cause failure of the specific three diesels. Without understanding the interplay between the diesels and the ESW system, this important asymmetry would be missed.

6.3.2. Example 2 - Environmental Asymmetry

Consider the set of four valves shown in Figure 2; they are normally closed valves in the suction line from the sump to the low pressure injection pumps in a PWR. One of the suction paths is required to open when it is necessary to go to low pressure recirculation following a LOCA.

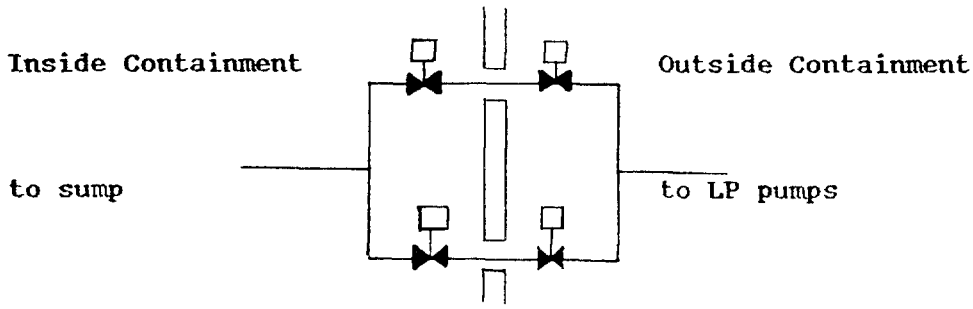

FIG. 2. Set of four valves

In some sense the group of valves is homogeneous, they are of the same design, and tested the same way with the same frequency. However, there are environmental differences; two of the valves are inside containment, and two are outside. One might assume that under normal circumstances this difference is not significant, particularly as the valves inside containment are qualified for a much harsher environment than the normal environment. Consequently it might be argued that they constitute a common cause component group. The modelling of such a series-parallel system raises the question of whether to include all combinations of terms, or mainly the global term. Common cause failures of components in series tend to be non-conservative. However, in this case, there are two significant considerations that clarify how the modelling should be performed. Firstly, when they are required to open, the valves inside containment see a much harsher environment than those outside. While the valves are supported to be qualified for this environment, it is not clear that their failure probabilities will be the same. Secondly, there is a possibility for some sequences to manually open the valves outside containment, which is not the case for those inside containment. Therefore for the accident conditions the two valves inside containment should probably be treated as a separate CCF component group.

6.3.3. Example 3 - Operational Asymmetry

Yet another example results in modelling the common cause failure of the safety relief valves in a BWR. There are many of these valves (typically in the order of 14 or so) and a large number have to fail to lead to loss of the depressurization function. Because of the lack of data on high multiplicity groups of components, it is necessary to understand how the system is engineered and operated, in order to avoid unrealistically high common cause failure probabilities. One approach that has been used was based on asymmetry to argue, subjectively, for lower failure probabilities. The asymmetry was that which resulted from the maintenance policy of the plant where one-third of the valves were stripped down and rebuilt every refuelling outage. This results, therefore, in an asymmetry of the valves with respect to the state of degradation as a result of the environment in which they are located. Therefore, for failure causes associated with degradation, the valves are divided into three separate common groups with a less than complete coupling between the groups. Since it was judged from looking at failure event data that the failure modes of such valves were dominated by causes that can be attributed to gradual deterioration, a lower common cause failure probability than would otherwise be assigned was judged to be acceptable. This type of asymmetry is, therefore, dealt with in a different way, by its incorporation in the estimation of a common cause probability, rather than being represented explicitly in the model.

REFERENCES

Bento, J.-P. et al. (1985) Reliability Data Book for Components in Swedish Nuclear Power Plants, prepared by ABB Atom AB and Studsvik AB for Nuclear Safety Board of the Swedish Utilities and Swedish Nuclear Power Inspectorate.

Bertucio, R. et al. (1987) Analysis of Core Damage Frequency from Internal Events: Surry Unit 1, NUREG/CR-4550 Vol. 3, US Nuclear Regulatory Commission, Washington DC.

Dörre, P. (1989) Basic Aspects of Stochastic Reliability Analysis for Redundancy Systems, Reliab. Eng. Syst. Saf. **24**, 351-375.

Fleming, K.N. and Mosleh, A. (1985) Classification and Analysis of Reactor Operating Experience Involving Dependent Events, EPRI NP-3967 prepared for Electric Power Research Institute by Pickard, Lowe and Garrick, Inc.

Gano, D.L. (1987) Root Cause and How to Find It, Nucl. News **30** 10 39-43.

Himanen, R., Kosonen, M. and Mankamo, T. (1989) "Defences against Common Cause Failures. Introduction to Quantitative Approach", In Proceedings of the 10th Annual Symposium of the Society of Reliability Engineers, Scandinavian Chapter, Stavanger, Norway, Elsevier Applied Science, London and New York.

Hirschberg, S. (Ed.) (1990) Dependencies, Human Interactions and Uncertainties in Probabilistic Safety Assessment, Final Report of the NKA Project RAS 470, Nordic Liaison Committee for Atomic Energy.

Hirschberg, S. (Ed.) (1987) NKA-project "Risk Analysis" (RAS-470): Summary Report on Common Cause Failure Data Benchmark Exercise, Final Report RAS-470 (86) 14 (ABB Atom Report RPA 86 - 241).

Hirschberg, S., Björe, S. and Jacobsson, P. (1989) "Retrospective Quantitative Analysis of Common Cause Failures and Human Interactions in Swedish PSA Studies", In Proceedings of PSA '89 - International Topical Meeting on Probability, Reliability and Safety Assessment, American Nuclear Society, La Grange Park, IL.

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

IAEA (1992) Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants, Safety Series, IAEA, Vienna.

Mankamo, T. and Kosonen M. (1988) "Dependent Failure Modelling in Highly Redundant Structures - Application to BWR Safety Valves", In Proceedings of the 9th Annual Symposium of the Society of Reliability Engineers, Scandinavian Chapter, Västeras, Sweden, October 10 - 12, 1988.

Mosleh, A., Fleming, K.N., Parry G.W., Paula H.M., Rasmuson D.M., and Worledge D.H. (1988, 1989) Procedures for Treating Common Cause Failures in Safety and Reliability Studies, NUREG/CR-4780, EPRI NP-5613, Electric Power Research Institute, Palo Alto, CA., Vol. 1 (1988), Vol. 2 (1989).

Mosleh, A. and Siu, N.O.(1987), "A Multi-parameter, Common-Cause Failure Model", In Transactions of the 9th International Conference on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, Vol. M, A.A. Balkema, Rotterdam/Boston.

Paula, H.M. and Parry G.W. (1990) A Cause-Defense Approach to the Understanding and Analysis of Common Cause Failures, NUREG/CR-5460, SAND89-2368, US Nuclear Regulatory Commission, Washington, D.C.

Poucet, A., Amendola A. and Cacciabue P.C. (1987) CCF-RBE, Common Cause Failure Reliability Benchmark Experience, Report EUR 11054EN, Commission of the European Communities, Joint Research Centre, ISPRA Establishment.

Rasmuson, D. et al., (1982) Use of COMCAN III in System Design and Reliability Analysis, EGG-2187, EG&G Idaho, Inc., Idaho Falls, Idaho.

Smith, A.M. et al., (1988) Defensive Strategies for Reducing Susceptibility to Common Cause Failures, EPRI NP-5777, Electric Power Research Institute, Palo Alto, CA.

CONTRIBUTORS TO DRAFTING AND REVIEW

Consultants Meeting on Guidelines on Common Cause Failure
16-20 October 1989, Vienna

SWEDEN	S. Hirschberg	ABB Atom AB S-72163 Västeras
UNITED STATES OF AMERICA	G. W. Parry	Halliburton NUS Environmental Corp. 910, Clopper Road Gaithersburg MD 20878-1399
IAEA	L. Carlsson	Scientific Secretary

Reviewed by:

FINLAND	T. Mankamo	Avaplan Oy Kuunsade 2 DE SF-02210 Espoo
UNITED STATES OF AMERICA	A. Mosleh	Dept. of Nuclear Engineering University of Maryland College Park MD 20742
	W. E. Vesely	SAIC 655 Metro Place South Suite 745 Dublin, OH 4301