

**THE IMPACT OF MAINTENANCE PROGRAM CHANGES
ON COMMON CAUSE FAILURE RATES**

By

Meng Ouyang

S.B., Shanghai Jiao Tong University, China
(1982)

Submitted in Partial Fulfillment
of the Requirements for the Degree of

MASTER OF SCIENCE

IN

NUCLEAR ENGINEERING

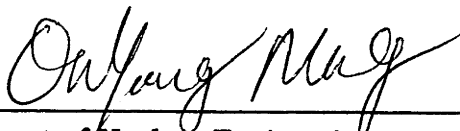
at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

January, 1992

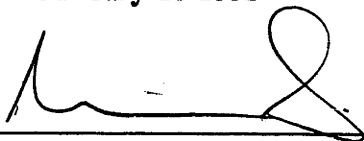
• Massachusetts Institute of Technology

Signature of Author



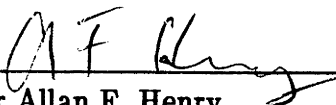
Department of Nuclear Engineering
January 16 1992

Certified by



Professor Nathan Siu
Thesis Supervisor, Department of Nuclear Engineering

Accepted by



Professor Allan F. Henry
Chairman, Department Committee on Graduate Students

ARCHIVES
MASSACHUSETTS INSTITUTE
OF TECHNOLOGY

JUN 23 1992

LIBRARIES

**THE IMPACT OF MAINTENANCE PROGRAM CHANGES
ON COMMON CAUSE FAILURE RATES**

By

Meng Ouyang

Submitted to the Massachusetts Institute of Technology Department of Nuclear Engineering on January 1992, in partial fulfillment of the requirements of the Degree of Master of Science in Nuclear Engineering.

ABSTRACT:

This study develops an approach to assess the impact of maintenance program changes on Common Cause Failure (CCF) rates. The approach involves the following tasks: (1) identify the common cause basic event of interest; (2) classify and screen historical events involving common cause component group; (3) analyze root causes and coupling mechanisms of historical events; (4) assess applicabilities of those root causes and coupling mechanisms to the plant being analyzed; (5) assess final event impact vectors and apply α -factor common cause failure model to calculate the failure rate of the common cause basic event .

In this study, the common cause failure of four RHR system pumps in the James A. Fitzpatrick nuclear power plant is taken as the basic event of interest. Case study analyses shows that there can be a two order magnitude of variation in the CCF rates between best maintenance practices and the worst maintenance practices. Propagation of these CCF rate changes through the plant risk model shows that the associated plant risk variation is around a factor of 2.

Thesis Supervisor: Nathan Siu
Title: Associate Professor of Nuclear Engineering

ACKNOWLEDGEMENTS

I acknowledges with gratitude to Professor Nathan Siu for his professionally valuable advice and suggestions during the course of this investigation. His constant encouragement and inexhaustible patience are greatly appreciated. Without his supervision, this work would not be possible.

I am also very thankful to Professor N. Rasmussen for his valuable advice and interests.

Thanks are also due to New York Power Authority for its financial support throughout this project.

I am also thankful to my colleagues, R. Su, W. He and K. Credit, for their informative and stimulating discussions during the course of this investigation. Many thanks are also due to Anne Hudson for her help in using T³.

For her tremendous encouragement and love throughout these years, I am very grateful to my wife XiaoXia.

And last, I would like to express my gratitude to my parents for their constant support and encouragement.

TO MY DARLING: XIAOXIA

TABLE OF CONTENTS

	Page
ABSTRACT	2
ACKNOWLEDGEMENT	3
TABLE OF CONTENTS	5
LIST OF TABLES	7
LIST OF FIGURES	8
1. INTRODUCTION	9
1.1 Background	9
1.2 Maintenance In PRA Models	10
1.2.1 Maintenance Contributions to Component Unavailability	11
1.2.2 Maintenance Contributions to System Unavailability	14
1.2.3 Current Modeling of Parameters Affecting Maintenance Unavailability	16
1.2.3.1 Modeling the Standby Failure Rate λ_s	16
1.2.3.2 Modeling Human Error Rate ϕ_{he}	18
1.2.4 Modeling Maintenance Impact on Common Cause Failure Parameters	20
1.2.5 Identification of Problem Area	25
1.3 Approach	25
1.4 Overview of the Thesis	27
2. MODELING MAINTENANCE IMPACT ON CCF RATES	
2.1 General Procedure for Calculating CCF Rates	32
2.1.1 Step 1 – Define Common Cause Basic Event	33
2.1.2 Step 2 – Select Probability Model	34
2.1.3 Step 3 – Classify and Screen CCF Event Data	35
2.1.4 Step 4 – Estimate Probability Model Parameters	36
2.2 Development of Screened RHR Pump Failure Event Data Base	39
2.2.1 Data Sources	39
2.2.2 Selection of Events	39
2.2.3 RHR Pump Failure Mechanisms	41
2.2.3.1 Root Causes	41
2.2.3.2 Coupling Mechanisms	43
2.3 Modeling Maintenance Impact on CCF Rates	43
2.3.1 Initial Impact Vectors for Actual Event	44
2.3.2 Degree of Applicability to JAF	45
2.3.3 Mapping Up and Mapping Down	55
2.3.4 Estimation of CCF Parameters	55

TABLE OF CONTENTS

	Page
3. QUANTIFYING MAINTENANCE IMPACT ON RISK: CASE STUDIES	79
3.1 Maintenance Program Block Options	79
3.1.1 Block 1 – Maintenance Management	80
3.1.2 Block 2 – Corrective, Preventive and Predictive Maintenance	80
3.1.3 Block 8 – Personnel Quantification and Training	81
3.1.4 Block 9 – Procedure and Regulatory Constrains	82
3.2 Effect of Maintenance Program Changes on Q_k	82
3.3 Effect of Maintenance Program Changes on Risk	83
4. CONCLUDING REMARKS	88
4.1 Summary of Results	88
4.2 Issues and Limitation	89
4.3 Applications	89
4.4 Future Work	90
REFERENCES	91
APPENDIX A: Descriptions of Comprehensive Maintenance Program Blocks	93
APPENDIX B: Maintenance Program at J.A. Fitzpatrick Nuclear Power Plant	98
APPENDIX C: James A. Fitzpatrick Plant Risk Model	103

LIST OF TABLES

	Page
Table 2.1	58
Table 2.2	60
Table 2.3	61
Table 2.4	63
Table 2.5	64
Table 2.6	65
Table 2.7	67
Table 2.8	69
Table 2.9	70
Table 2.10	70
Table 2.11	70
Table 2.12	71
Table 2.13	72
Table 2.14	73
Table 2.15	73
Table 2.16	73
Table 2.17	74
Table 2.18	75
Table 2.19	76
Table 2.20	77
Table 3.1	85
Table 3.2	87

LIST OF FIGURES

		Page
Figure 1.1	Time-Dependent Component Unavailability	28
Figure 1.2	Time-Dependent Unavailability of a Two-Component System	29
Figure 1.3	Decision Tree for Assessing and Mapping Event Impact Vectors	30
Figure 1.4	Figure Chart of the Research Approach	31
Figure 2.1	RHR Pump 'FS' Mode Failure Mechanisms	62
Figure 2.2	Approach For Quantifying CCF Parameters	66
Figure 2.3	Approach For Quantifying CCF Event "Applicability"	68
Figure A.1	Comprehensive Maintenance Program Block Diagram	97

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

In a nuclear power plant, numerous engineering safeguards are used to defend against the accidental release of radioactive materials. However, plant safety still ultimately depends on the ability of plant staffs to properly operate and maintain the plant. Improvements in plant maintenance will lead to increased plant safety. However, the risk impacts of changes in maintenance activities, needed to determine whether a given change actually represents an improvement, are not as well understood. Thus, for example, although it may be known that reducing the frequency of surveillance testing may actually reduce the wear on a given component and reduce costs both in labor and equipment, the quantitative increase in component reliability and the associated decrease in plant risk are not usually known.

In principle, the quantitative impact of maintenance actions on risk are incorporated in a Probabilistic Risk Assessment (PRA) through the following two groups of parameters: 1) the equipment failure parameters, e.g., the independent and common cause component failure rates, and 2) maintenance related parameters, e.g., maintenance frequency and durations. In recent years, researchers have developed methods to quantitatively relate the second group of parameters with plant risk and system unavailability. These methods have been applied in the assessment of the change in risk associated with changes in Allowed Outage Times

(AOTs) and Surveillance Testing Intervals (STIs) as specified in the Technical Specifications for a given plant. The AOTs specify the amount of time a plant may operate in a potentially vulnerable configuration (due to the failure of specified component) before it must be shutdown; the STIs specify the frequency at which equipment surveillance tests must be performed.

On the other hand, studies that quantitatively relate maintenance practices with equipment failure parameters, system unavailability and plant risk have only recently been initiated. The purpose of this project is to model the impact of maintenance activities on this group of PRA parameters.

1.2 MAINTENANCE IN PRA MODELS

Maintenance actions on a component can affect component unavailability in a number of ways. First, the component can be rendered unavailable for a certain duration. Second, the component can be improperly restored upon completion of maintenance. Third, a component failure can be induced by improper maintenance. Fourth, on the positive side, the maintenance actions can, in principle, change the failure parameters for the component; effective maintenance can reduce the failure rate of a component subject to aging. Fifth, also positively, failures occurring while a system is in standby can be detected.

By affecting component unavailability, maintenance will also clearly affect system unavailability. The degree of impact will depend on a number of factors, including the degree of redundancy and the particular scheme used to schedule testing and maintenance.

This section briefly discusses conventional models used to treat the effect of maintenance on component unavailability and advanced modeling efforts aimed at

better treating the effect of maintenance on system unavailability.

1.2.1 Maintenance Contributions to Component Unavailability

Component unavailability models vary according to whether the component is normally running or on standby. In the former case, it is clear when a component fails; renewal theory shows that the average unavailability for a normally running component is (assuming that the component is restored to "as-good-as-new" conditions after maintenance) given by [1]:

$$Q_r = \frac{\tau_r}{\tau_f + \tau_r} \quad (1.1)$$

where τ_f is the expected failure time (i.e., the "mean time to failure") and τ_r is the mean repair time (i.e., the "mean time to repair"). Here, it can be seen that maintenance activities enter primarily through the repair term τ_r , although improved maintenance should affect the failure term τ_f also. Time-dependent unavailability models can be developed using Markov modeling techniques (e.g., see [2]), but are not generally used in current PRA studies.

In the case of standby components, the failure may not be detected until the next demand, test, or surveillance. A simple plot for the time-dependent unavailability of a standby component is shown in Figure 1.1. This plot assumes that the component is unavailable during the testing/maintenance period $(T - \tau_{tm}, T)$. Immediately following testing and maintenance, the time-dependent component unavailability is very small (it is non-zero since there remains a finite probability that the component will fail to start on demand, possibly because the maintenance is performed incorrectly). The unavailability increases with time, as

there is increasing likelihood that the component will fail, until the next maintenance period. Note that, in principle, the unavailability growth between maintenance periods can vary; this reflects the opposing effects of aging and maintenance on the component failure parameters (e.g., the standby failure rate λ_s). However, if λ_s is constant and if $\lambda_s(T - \tau_{tm})$ is small, the time-dependent unavailability for a standby component can be simply written:

$$Q_s(t) = \begin{cases} Q_d + \lambda_s t & 0 \leq t \leq T - \tau_{tm} \\ 1 & T - \tau_{tm} \leq t \leq T \end{cases} \quad (1.2)$$

where Q_d represents component unavailability on demand (including the possibilities that there is an undetected failure, possibly from a human error during system restoration, and that the component fails on demand). Using the definition for average unavailability over a time period $(0, T)$:

$$Q \equiv \frac{1}{T} \int_0^T Q(t) dt \quad (1.3)$$

the average unavailability for the standby component over the interval $(0, T)$ is then approximately given by

$$Q_s \doteq Q_d + \frac{\lambda_s T}{2} + \frac{\tau_{tm}}{T} \quad (1.4)$$

(assuming that $T \gg \tau_{tm}$). Note that it is common practice in PRA to separate the contributions of hardware failures and human errors to the demand unavailability Q_d [3], and that separate testing and maintenance contributions to τ_{tm} are also often

distinguished. Thus, for intervals $(0, T)$ in which multiple tests and/or maintenance actions are allowed,

$$Q_s \doteq \phi_h + \frac{\lambda_s T}{2} + f_t \tau_t + f_m \tau_m + Q_{he} \quad (1.5)$$

where ϕ_h is the demand failure probability (for hardware failures), f_t is the frequency of tests (per unit time), τ_t is the average duration of tests, f_m is the frequency of maintenance actions (per unit time), τ_m is the average duration of maintenance actions, and Q_{he} is the unavailability of the component due to human errors.

It should be pointed out that Eq. (1.5) applies only when one type of testing and one type of maintenance are performed. However, the generalization of this model to handle a variety of tests and maintenance actions is clear.

A slightly more complicated model for standby component unavailability is presented in Ref. 4. In this model, when a component is undergoing maintenance, there is a finite probability that the component can function properly when demanded (i.e., the test/maintenance function can be overridden). This covers cases where even if a component is aligned in a testing configuration, it can realign when a demand signal is received. Note that upon overriding the maintenance function, there is a possibility that the component will fail to operate on demand.

As in the simple model of Eqs. (1.2) and (1.5), the component can fail while on standby. In this model, however, the possibility that the failure can be detected and repaired before the next scheduled testing/maintenance period is treated. In such cases, the repair time can be treated explicitly as a random variable, or can be conservatively assumed to be equal to the associated Allowed Outage Time (AOT).

1.2.2 Maintenance Contributions to System Unavailability

The simple models described in the previous section quantify the time-dependent and average unavailabilities of a single component. The time-dependent and average unavailabilities of standby systems and normally operating systems depend not only on the component unavailability, but also the degree of redundancy within the system (with respect to the component of interest) and the system operating procedures. The procedures, for example, determine how long a component can be unavailable before the plant must be shut down (i.e., they provide the Allowed Outage Times).

The system time-dependent and average unavailabilities also depend on the particular testing/maintenance scheme used. There are three general test/maintenance schemes that can be envisioned:

- i) simultaneous testing/maintenance,
- ii) sequential testing/maintenance, and
- iii) staggered testing/maintenance.

The last scheme is similar to the sequential scheme, except that the testing/maintenance actions on redundant components/trains are separated by some time interval (rather than having one action immediately succeed another).

Given the particular testing/maintenance scheme, the calculations for system unavailability can be accomplished analytically for simple systems. Consider, for example, two identical, redundant standby components under a sequential testing scheme (see Figure 1.2). The time-dependent unavailability of the system is given by

$$Q_{sys}(t) = \begin{cases} (Q_d + \lambda_s t)^2 + (Q_{ccf} + \lambda_{ccf} t) & 0 \leq t \leq T - 2\tau_{tm} \\ (Q_d + \lambda_s t) & T - 2\tau_{tm} \leq t \leq T \end{cases} \quad (1.6)$$

where, as in Eq. (1.2), the Q_d term includes hardware failures and human error, and the subscript "ccf" denotes common cause failure. The term τ_{tm} is the duration of the testing/maintenance period for one component. Note that the second line in Eq. (1.6) treats the conditional unavailability of one component, given that the other component is unavailable due to testing/maintenance.

Using Eqs. (1.3) and (1.6), the average unavailability for this system is approximated by (assuming that $\tau_{tm} \ll T$):

$$Q_{sys} \doteq \left\{ [Q_d^2 + Q_d(\lambda_s T) + \frac{(\lambda_s T)^2}{3}] + (Q_{ccf} + \frac{\lambda_{ccf} T}{2}) \right\} + (Q_d + \frac{\lambda_s T}{2}) (\frac{2\tau_{tm}}{T}) \quad (1.7)$$

Note that if the dependence between the components is ignored, there would result:

$$Q'_{sys} \doteq \left\{ [Q_d^2 + Q_d(\lambda_s T) + \frac{(\lambda_s T)^2}{4}] + 2(Q_d + \frac{\lambda_s T}{2}) (\frac{\tau_{tm}}{T}) + (\frac{\tau_{tm}}{T})^2 \right\} \quad (1.8)$$

The last term, which treats a fictitious contribution due to simultaneous maintenance, is likely too small to account for the lack of treatment of common cause failure [as represented correctly in Eq. (1.7)]. Comparing Eqs. (1.7) and (1.8), it can be seen that system unavailability due to testing/maintenance must be treated at the system (fault tree) level, rather than at the component level.

1.2.3 Current Modeling of Parameters Affecting Maintenance Unavailability

Changes in a maintenance program can affect the unavailability of components and systems through the parameters of Eqs. (1.5) and (1.8). More specifically, these parameters are ϕ_h , λ_s , Q_{ccf} , λ_{ccf} , Q_{he} , f_t , τ_t , τ_m , and T . Some changes can be modeled very simply. Increases in the frequency of testing and maintenance, for example, can be treated by increasing f_t and τ_t in Eq. (1.5) and reducing T (since increased testing and maintenance leads to a reduced detection time and a reduced likelihood of standby failures). Other changes, however, require more analysis. Since this work is more closely related with common cause failure modeling, the parameters Q_{ccf} and λ_{ccf} are given a detailed discussion in Section 1.2.4. Previous research related to the parameters ϕ_h , λ_s and Q_{he} are briefly discussed in the following subsections.

1.2.3.1 Modeling Maintenance Impact on the Parameter ϕ_h , λ_s

The term, ϕ_h , can be argued to be incorporated (at least to some extent) in the treatment of λ_s , since both "standby failures" and "failures on demand" are observed (barring tests) at the time of demand. Indeed, most plant-level PRA studies lump these two failures together. In principle, the standby failure rate λ_s can vary between maintenance periods, due to the competing effects of aging and maintenance. A significant amount of work has been done on the issue of aging; work aimed at quantifying the impact of maintenance on λ_s has only recently been initiated. In standard PRA analyses, the failure rates for components are assumed

to be constant over time. (Equivalently, failures are assumed to be random events governed by a Poisson process.) This model corresponds to the constant failure rate portion of the well-known bathtub "curve." To accommodate aging effects, the failure rate must be allowed to vary as a function of time. In Ref. 5, the linear aging model described in Ref. 6 is implemented in a time-dependent fault tree program (FRANTIC-LA) to compute the effects of component aging on system availability. Ref. 5 applies this model to periodically tested components. It allows different treatment of renewal options, allows the user to change component aging parameters during plant life. In turn, this allows the modeling of different aging scales for every component, the time when the component was subject to any significant maintenance or repair action, and the time when the component was replaced with a new one. In addition to different renewal options, Ref. 5 allows detailed modeling of the test and repair processes. Ref. 5 also studies the impact of testing and maintenance on the aging-related unavailability of piping systems. It shows that good-as-new testing and repair have the maximum effectiveness with regard to detecting and correcting aging contributions. Two other renewal strategies also shown to be capable of controlling aging effects: good-as-old testing with good-as-new repair, and periodic replacement of aging components. The study shows that the testing effectiveness and frequency are very significant parameters in controlling aging effects, even when the testing only returns the component to a good-as-old condition.

Ref. 7 studies core melt frequency changes due to aging. Changes in the component unavailabilities, structure failure probabilities, and initiating event frequencies are related to the aging rate and plant maintenance policy using a linear aging model. In Ref. 7, the component is assumed to be restored to as good as new

conditions after a time period L . To account for the possibility that the overhaul is not completely efficient, the scheduled overhaul interval can be replaced by an "effective overhaul interval". To account for the possibility that the surveillance is not completely efficient in detecting aging effects, an "effective surveillance interval" can be used. Assessments of efficiency are made based on the maintenance practices employed at the time of the analysis.

As mentioned earlier, work on evaluating the effect of maintenance on the failure parameters used in a PRA is more recent. Ref. 8 discusses a quantitative methodology to assess the reliability and risk benefits of maintenance. This work employs a Markov model that treats a variety of component states: working, degraded, under maintenance, and failed. This model addresses the primary problem with the current data base when attempting to quantify the impact of maintenance on failure parameters: the failure data are generally too scarce. By including other states for which more data are available, the model of Ref. 8 can provide a more robust analyses of maintenance effectiveness. Such analyses can be used when responding to the Maintenance Rule.

Ref. 8 evaluates the impact of variations in AOTs treating both positive and negative impacts. The results show that using the Markov model, the predicted effects of a rolling maintenance program on component unavailability can be significant (greater than a factor of 10), and that optimal maintenance regions can be identified.

1.2.3.2 Modeling Maintenance Impact on Parameter Q_{he}

A number of models have been developed for human reliability analysis.

Human error could appear both in operating and maintenance activities. Ref. 9 describes a model developed especially for analyzing human reliability in maintenance activities. This model is called Maintenance Personnel Performance Simulation (MAPPS). MAPPS is an ability-driven, group-oriented, stochastic simulation model. It simulates the maintenance tasks through the use of three types of input data: variable, task and subtask. Variable parameters describe the conditions of the environment and characteristics of the workers. Task and subtask parameters describe the maintenance job to be performed. The model provides algorithms to modify the technicians' basic ability levels as a function of their current states and the working conditions. Those include technician's fatigue, environmental temperature, technician's level of aspiration, etc. The difference between total ability available and ability required is then used as one of four components in computing the task success probability. This model uses information on maintenance tasks and maintenance personnel to calculate the task success probability.

Another widely used human reliability model is the Technique for Human Error Rate Prediction (THERP) [10], which is representative of models used in PRAs. This model can be used both for operating conditions and maintenance conditions. It is also a task oriented model. It employs a Human Reliability Analysis Tree (HRA Tree) to model the structure of the task. The major feature of this model is its 27 data tables used for the assignment of failure rates for each branch of the HRA Tree developed for the particular task. In those tables, generic failure rates are provided for personnel actions during operations and/or maintenance. For modeling the human error rates at a particular plant, an assessment of the difference between the average level (defined in the tables) and actual practice levels

has to be performed. This information is used to modify the corresponding generic failure rates before they are put into the HRA Tree to generate the task failure rate (or human rate). Assessment of the dependency between each step in the task is also another required steps in the use of this model. This dependency assessment relies heavily on the analyst's assessment of the effectiveness of current plant operating and maintenance programs and his assessment of personnel qualifications.

In Ref. 11, an approach is developed to quantify the impact of maintenance program changes on one PRA model parameter, the frequency that operators fail to correctly restore equipment after maintenance (ϕ_{re}). This approach use Human Reliability Tree and Dependence Level Tree to help quantify the ϕ_{re} . Different maintenance activities are considered in developing and quantifying those trees.

1.2.4 Modeling Maintenance Impact on Common Cause Failure Parameters

Q_{ccf} , the common cause failure on demand and λ_{ccf} , the common cause standby failure rate are the two parameters used in Eq.(1.7) to account for the system unavailability contribution of standby common cause failure. Similar to the definition of Q_d for single component, Q_{ccf} includes hardware failures and human errors. In current common cause failure probability models (discussed in the following sections), the term Q_{ccf} and λ_{ccf} are lumped together during the analysis.

As defined in Ref. 12, in the context of system modeling, common cause events are a subset of dependent events in which two or more component fault states exist at the same time, or in a short time interval, and are a direct result of a

shared cause. It is also implied that the shared cause is not another component state because such cascading of component states is normally due to a functional coupling mechanism. Such functional dependencies are normally modeled explicitly in system models without the need for special common cause event models. In recent years, many models have been developed to treat common cause events. These models include the binomial failure rate model, the multiple Greek letter model, the beta factor model and its advanced version, the alpha factor model , and many other models. Each model has its own set of parameters which have to be estimated before the model can be used to calculate CCF rates.

In Ref. 12, a four-stage general approach for including common cause failures in a PRA study is presented. These four stages are:

1. System Logic Model Development.
2. Identification of Common Cause Component Groups.
3. Common Cause Modeling and Data Analysis.
4. System Quantification and Interpretation of Results.

For Stage 3, common cause modeling and data analysis, a four-step procedure is developed. Those steps include:

- A. Definition of Common Cause Basic Events. Usually these events are determined by the requirements of system modeling.
- B. Selection of Probability Models for Common Cause Basic Events.
Ref. 28 discusses several single parameter and multiple parameter

probability models. It points out that among all models, the alpha factor model is more consistent with the event oriented approach developed in Ref. 28, and easily generates more precise results because it makes maximum possible use of system based failure events. Other probability models, including beta factor model, are component failure based models.

- C. **Data Classification and Screening.** Due to the rarity of common cause events and the limited experience for individual plants, the amount of plant-specific data for common cause analysis is very limited. Therefore, in almost all cases, data from the industry experience and a variety of sources have to be used to make statistical inferences about the frequencies of the common cause events. However, due to the fact that there is a significant variability in plants, especially with regard to the coupling mechanisms and defenses against common cause events, the industry experience is not, in most cases, directly applicable to the specific plant being analyzed. Equally important, the analysis boundary conditions that indicate what category of components and causes should be analyzed, requires careful review and screening of event to ensure consistency of the data base with the assumptions of the system model. Ref. 12 employs an Event Impact Vector Assessment approach to assist this data base development. Figure 1.3 shows this approach. The output of this approach is an average impact vector which is used by probability models to generate common cause failure rates.

The important feature of this approach is the assessment of applicability of the event to the plant being analyzed. This applicability

treats: 1) the degree the failure mechanisms underlying an event are applicable to the plant being analyzed; 2) physical differences between the plant experiencing the event and the plant being analyzed. Ref. 12 points out that this applicability assessment needs a considerable amount of judgment to treat the effectiveness of the common cause defensive tactics in the plant being analyzed. Appendix A of Ref. 12 categorizes those defensive tactics as follows:

- **Barriers:** Any physical impediment that tends to confine and /or restrict a potentially damaging condition.
- **Redundancy:** Additional, identical, redundant components added to a system for the purpose of increasing the likelihood that a sufficient number of components required to perform a given function will survive exposure to a given cause of failure.
- **Personnel Training:** A program to ensure that the operators and maintenance personnel are familiar with procedures and are able to follow them during all conditions of operation.
- **Quality Control:** A program to ensure that the product is in conformance with the documented design.
- **Preventive Maintenance :** A program of applicable and effective maintenance tasks designed to prevent premature failure or degradation of components.
- **Monitoring, Surveillance Testing and Inspection.**
- **Procedure 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: Diversity in staff(i.e., using different teams to install, maintain, and/or test redundant trains); Functional diversity (i.e., using different approaches to achieve roughly the same results.); and equipment diversity.**

It can be seen that the maintenance program plays an important role in those defensive tactics because the last 6 categories generally belong to a maintenance program implemented in a plant. The maintenance impact on common cause failure could at least be qualitatively analyzed by comparing the effectiveness of a maintenance program in the plant being analyzed with the observed failure mechanisms for the data base events. How to quantitatively assess the effectiveness remains a problem to be addressed.

- D. The final step for data classification and screening is the estimation of probability model parameters using the average impact vectors obtained in the last step.**

Ref. 13 aims at understanding common cause failures by emphasizing the development of general defensive tactics to common cause failures in an plant. The maintenance program, according to Ref. 13, is a part of that defense system. Ref. 13 employs the beta-factor CCF probability model in its analysis. Its main feature is the use of failure rate modifiers to account for the effectiveness of different defensive tactics against different root causes. Those modifiers are applied to beta-factor model parameters directly, i.e. the total component failure rate and β . Thus it accounts for maintenance impact on common cause failures at the probability model level rather than at the data base level.

1.2.5 Identification of Problem Area

Conventional PRA methods are currently capable of quantifying the risk impact of certain maintenance program changes (e.g., changes in testing intervals). These models, however, do not address potential changes in the values of failure parameters (e.g., λ) associated with the maintenance program changes. Recent work on the modeling of component degradation and aging (e.g., [7,14]) shows considerable promise in addressing this issue. Ref. 13 analyzes the impact of some maintenance activities on common cause failures at the CCF probability model level. It does not, however, use the available data on CCF. This thesis constructs a systematic approach for assessing the applicabilities of failure mechanisms of actual events, and uses the resulting modified CCF event data base to estimate the CCF model parameters.

1.3 APPROACH

In this study, an approach is developed to analyze the links between CCF rates and different maintenance practices. Figure 1.4 shows the flow chart for this approach. The upper portion of each box in the figure details the information sources and actions which are necessary to achieve the objective described in the lower portion of the box.

The approach involves the following tasks:

- Step 1. Identify the common cause basic event of interest. From a particular PRA study, the most risk important ranking of common cause failure

event could be identified. For this study, the common cause basic events of the interest are identified from the JAF plant PRA model.

- Step 2.** Classify and screen historical events involving common cause group components.
- Step 3.** Study the component failure mechanisms. Identify and classify root causes and coupling mechanisms. The root cause is the basic causal mechanism which leads to a component being unavailable or failed. The coupling mechanism is a characteristic of a group of components or piece parts that identify them as being susceptible to the same causal mechanisms of failure.
- Step 4.** Assess applicability of the root causes and coupling mechanisms for historical events to the plant being analyzed. Here, a systematic approach is developed to support this assessment. A comprehensive maintenance program is identified in Ref.11. It is provided in Appendix A and shown in Figure A.1. Maintenance program activities defined in those maintenance blocks are used as guidance for developing the assessment approach. The plant being analyzed is the JAF plant. Therefore it is necessary to understand current maintenance practices implemented in the JAF plant, and compare those practices with those of plants experiencing CCF failure events. Information on the JAF plant current maintenance practices are provided in Appendix B. The assessment approach uses failure rate modifiers defined in Ref. 13 to assess the effectiveness of different maintenance practices.
- Step 5.** Apply the results of Step 4 to estimate the parameters of the common cause failure probability model, and to calculate the failure rates of

common cause basic events. In this study, the alpha factor probability model is used for the CCF rates calculation. This model is chosen based on its advantages over the beta factor model in ease of use and completeness in modeling common cause failures.

1.4 OVERVIEW OF THE THESIS

Chapter 2 presents the modeling of impact of maintenance program changes on common cause failure rates. This modeling process is developed using the approach discussed in Section 1.3.

Chapter 3 presents case study analyses of CCF rate changes with variations in the JAF plant maintenance practices. Those case studies include: a baseline case reflecting the current plant maintenance practices; a best case assuming all maintenance activities implemented employ "best practices" (within the range of activities considered); and a worst case assuming all maintenance activities implemented employ "worst practices". Several other cases representing combinations of intermediate levels of maintenance activities between the best case and worst case are also analyzed.

Chapter 4 summarizes the research methodology and results, presents concluding remarks and points out the possible direction of future work.

Cases studies performed using the model developed in this thesis show that the common cause failure rates could be significantly reduced by an optimized maintenance program. The degree of CCF rate increase due to a partially degraded maintenance program is not as significant.

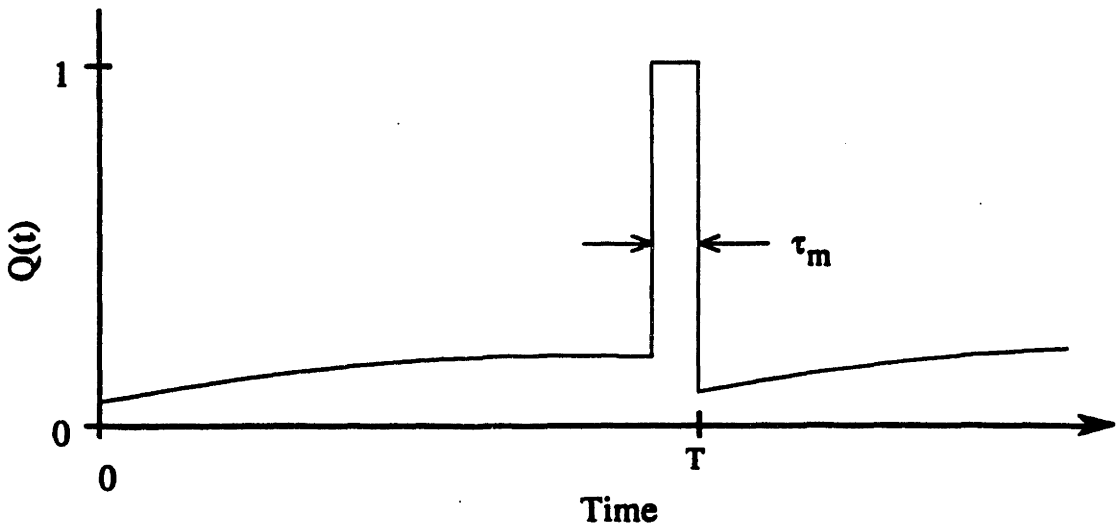


Figure 1.1 Time-Dependent Component Unavailability

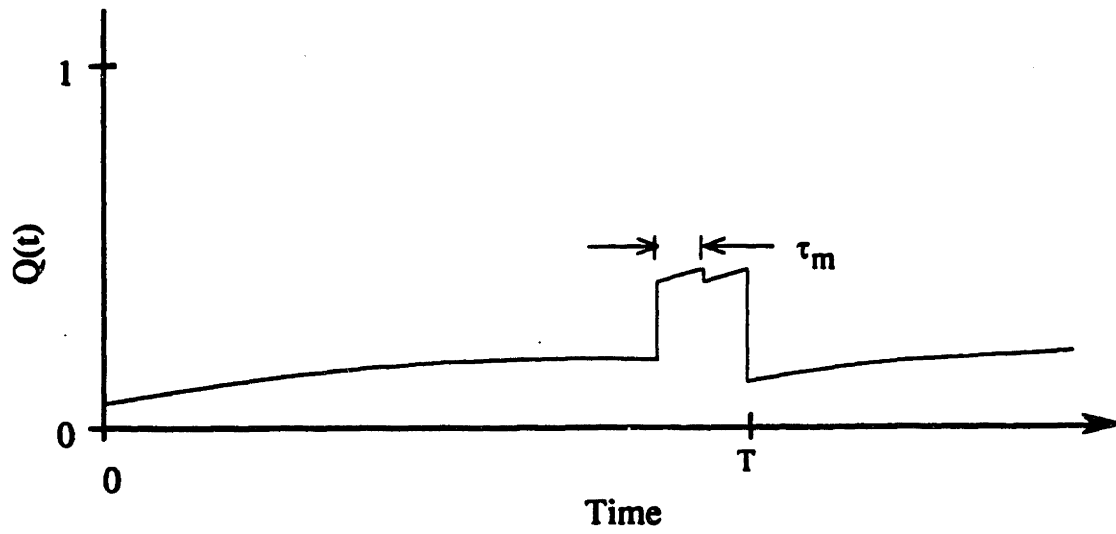


Figure 1.2 – Time-Dependent Unavailability of a Two-Component System

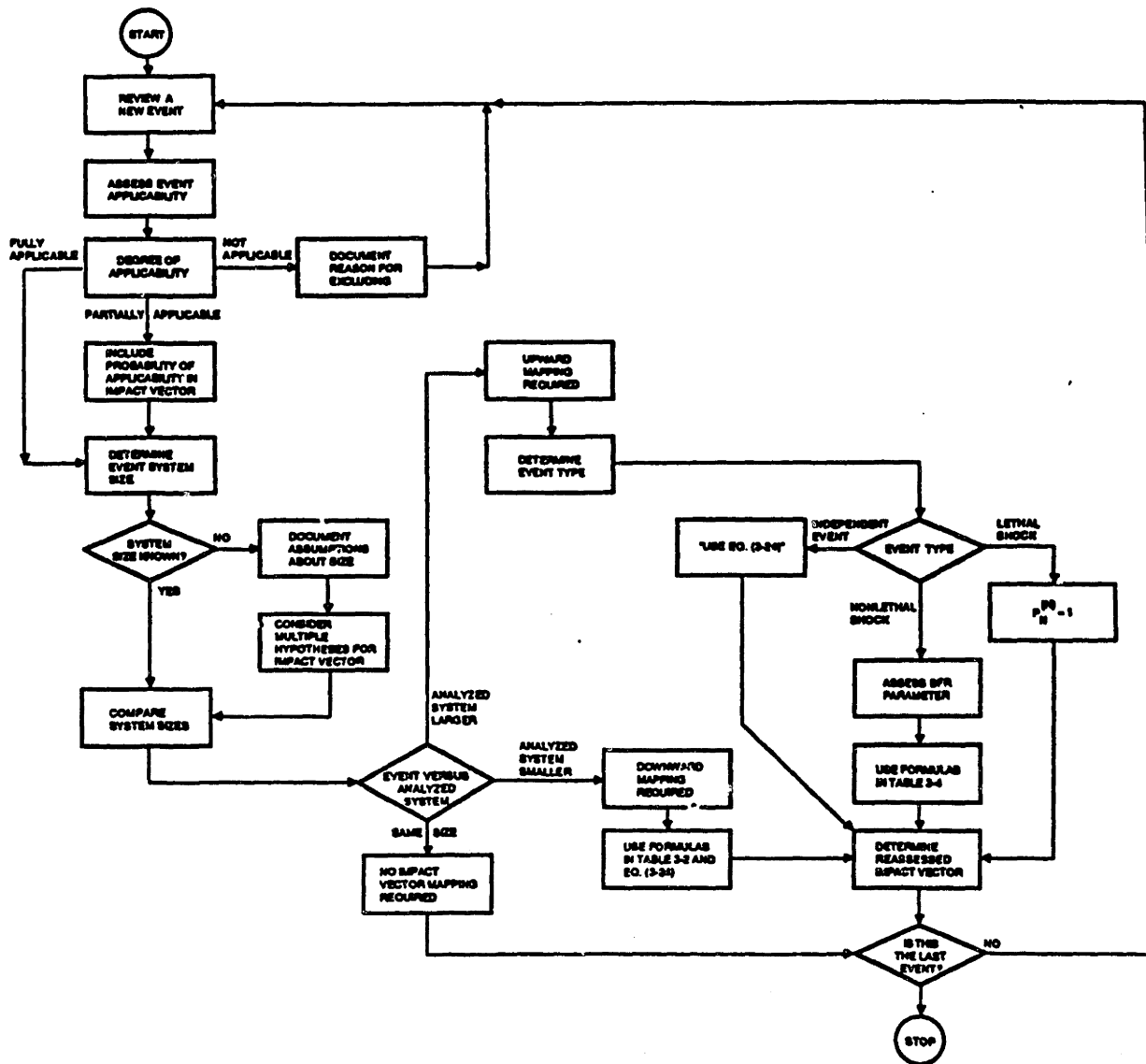


Figure 1.3 – Decision Tree for Assessing and Mapping Event Impact Vectors
 (from EPRI NP-5613, Vol.1. p. 3-44)

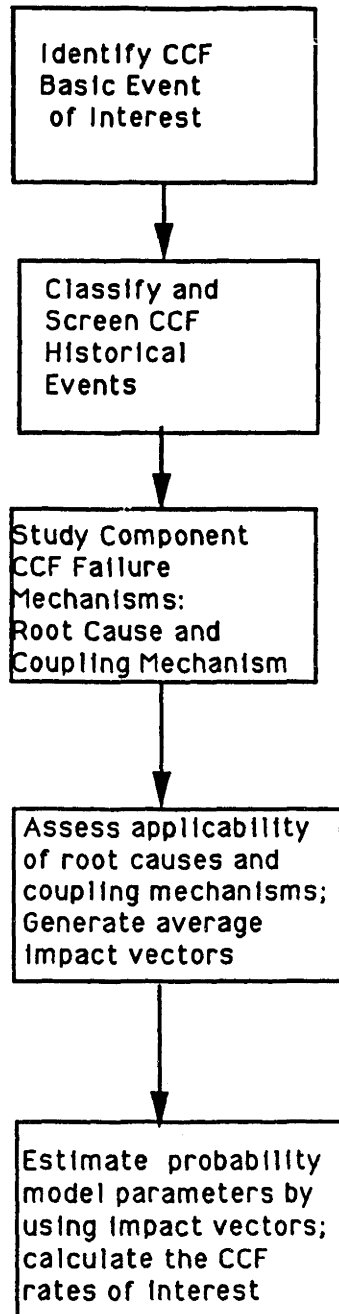


Figure 1.4 - Flow Chart of the Research Approach

CHAPTER 2

MAINTENANCE PROGRAM IMPACT ON CCF RATES

Ref. 11 is a maintenance program risk impact study focused on the James A. Fitzpatrick (JAF) nuclear power plant. In that study, the common cause failure (CCF) of 4 RHR pumps is identified as being the most important contributor to RHR system unavailability and a prime contributor to plant risk. CCF events have been found to be dominant risk contributors in many PRA studies as well. This chapter develops an approach for analyzing the effects of different maintenance practices on the likelihood of common cause failure. Since the CCF basic event to be analyzed involves RHR pumps of JAF plant, the current JAF maintenance practices are used at the "baseline" case for this approach. Chapter 3 applies this approach to a number of test cases which postulate different changes in the JAF maintenance program from the "baseline" case.

2.1 GENERAL PROCEDURE FOR CALCULATING CCF RATES

Ref. 12 presents a general approach for including common cause failures in a PRA study. (As noted earlier, "common cause failure analysis" refers to the statistical analysis of dependent failure events not explicitly modeled elsewhere in a PRA.) The approach employs four major stages:

- 1) System logic model development;
- 2) Identification of common cause component groups;
- 3) Common cause modeling and data analysis;
- 4) System quantification and interpretation of results.

This chapter focuses on the third stage, since the results of the first two stages are

incorporated in the JAF Individual Plant Evaluation study, and the fourth stage is the subject of Chapter 3 of this thesis.

According to Ref. 12, common cause modeling and data analysis in the third stage are accomplished using the following four steps:

- Define common cause basic events.
- Select probability model for common cause basic events.
- Classify and screen CCF event data.
- Estimate probability model parameters.

The following subsections discuss the application of these steps towards the analysis of the common cause failure of RHR pumps.

2.1.1 Step 1 – Define Common Cause Basic Event

In general, the objective of a CCF analysis is to quantify the frequency with which multiple components in a common cause failure group (which is usually composed of redundant, identical components in a system) fail due to the same cause. If there are m components in the group, the analysis is intended to estimate Q_k , the frequency with which k components ($k = 1, 2, \dots, m$) fail due to a single cause.

In this study, the basic event of interest is the failure of k motor-driven RHR pumps ($k = 1, 2, 3, 4$).

2.1.2 Step 2 – Select Probability Model

A number of probability models for CCF analysis are presented in Ref. 12. In particular, it describes both the β -factor model [15], which is used in the JAF IPE, and an improved version, the α -factor model [16], which is used in this study. As discussed in Refs. 12 and 16, the α -factor model has two advantages: a) it explicitly treats different levels of common cause failure events, and b) its parameters can be more easily estimated from available data. This latter advantage is due to the system-level orientation of the α -factor model, as opposed to the component-level orientation of the β -factor model.

Using the α -factor model, the frequencies of interest, Q_k , are computed as follows:

$$Q_k = \frac{m \alpha_k \phi_d}{\binom{m}{k} \alpha_t} \quad (2.1)$$

where

$\alpha_k \equiv$ fraction of RHR pump failure events involving the failure of k pumps ($k = 1,2,3,4$) due to a common cause

$\phi_d \equiv$ total demand failure rate for an RHR pump (runtime failures are neglected in this study, due to their low likelihood)

$\alpha_t \equiv$ a normalization factor, $\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4$.

$$\binom{m}{k} \equiv \frac{m!}{k!(m-k)!}$$

The value of the demand failure rate (ϕ_d) can be estimated from data (the number of failures divided by the number of trials), but is often obtained from standard sources of PRA parameter values. The values of the α_k are estimated from available CCF event data, as described in the next two subsections.

2.1.3 Step 3 – Classify and Screen CCF Event Data

In preparation for α -factor estimation, the available CCF event data are reviewed for their applicability to the problem at hand. Events judged to be inapplicable are "screened out" of the data base, i.e., they are not used in the estimation process.

Ref. 12 presents a number of general guidelines for screening events.

- Component-caused functional unavailabilities are screened out. It is assumed that multiple failures events in which one component failure is caused directly by the failure of another are directly modeled in the PRA. Note that the validity of this assumption depends on the modeling boundaries used (e.g., whether or not control circuits which can affect multiple components are treated separately or are included as part of the affected components).
- If a plant-specific defense exists that clearly precludes a class of CCF events, all specific events belonging to that class can be screened out.
- Events related to inapplicable plant conditions (e.g. pre-operational testing) can be screened out unless they reveal general causal mechanisms capable of occurring during power operation.
- If the event occurred during shutdown and would be restored before resuming power operation because of pre-service testing or if it cannot occur during power operation, the event is screened out.
- When considering multiple failure events, if the second failure happened after the first failure was dealt with, the failures are considered as being independent.
- Events regarding incipient failure modes (e.g., packing leaks) that clearly do

not violate component success criteria can be screened out.

- Only the events regarding the failure modes of interest are taken into consideration; events regarding failure modes that are irrelevant to the system logic model are screened out.

Due to the rarity of CCF events, the CCF parameter estimation process is quite sensitive to variations in the data base. The classification and screening task is therefore quite an important one. Section 2.2 discusses the performance of this task using available RHR pump CCF data.

2.1.4 Step 4 – Estimate Probability Model Parameters

In principle, the estimation of the α -factors is straightforward. Let n_k represent the number of failure events in the data base involving the common cause failure of k components. Then a maximum-likelihood point estimate for α_k is given by

$$\hat{\alpha}_k = \frac{n_k}{\sum_{i=1}^m n_i} \quad (2.2)$$

where m is the number of components in the common cause failure group. However, in practice, there may be significant uncertainty in the n_k [12,17].

To understand the sources of this uncertainty, it is important to recognize that the raw data used for CCF analysis generally consist of narratives of CCF events that have occurred in nuclear power plants. Furthermore, most of the events do not involve the plant being analyzed. These two points lead to uncertainties in

determining the n_k .

First, because the event narratives do not always provide enough detail, there can be significant uncertainty as to how many components were actually failed as a result of the event. Second, it is not clear if the event is applicable to the plant being analyzed, or, if it is applicable, what the level of impact of the event would be. In other words, even if the same initial common cause initiating fault arises, the number of components affected could vary. (Note that clearly inapplicable events are screened out of the data base, as described in the preceding subsection.) The second source of uncertainty is due to differences both in plant design and in plant operation and maintenance policies.

A three-step approach is used to quantify the α -factors, given the uncertainty in the CCF event data base [12]:

- i) Create an "impact vector" for each CCF event. For Event j in the data base, the impact vector is:

$$q_j = \{q_{0j}, q_{1j}, \dots, q_{kj}, \dots, q_{mj}\} \quad (2.3)$$

where q_{kj} is the probability that the j th event involved the common cause failure of k components. If the impact of the event is known with certainty, one q_k is assigned a value of unity and the others are assigned values of zero. For example in one event in the event data base, one RHR pumps failed to start on demand because of poorly connected fuse. The plant experiencing the event has only two RHR pumps. Thus, the impact vector for this event is $\{0,1,0\}$.

- ii) Modify the impact vectors to reflect the specific conditions at the plant being analyzed. This requires an assessment of the applicability of the event and an assessment of the magnitude of the event. Differences in system size are also treated. Ref. 12 describes "mapping up" and "mapping down" procedures that can be used to systematically account for differences in system size. The result is a set of modified impact vectors:

$$P_j = \{P_{0j}, P_{1j}, \dots, P_{kj}, \dots, P_{mj}\} \quad (2.4)$$

where p_{kj} is the probability that the j th event would lead to the common cause failure of k components at the plant being analyzed.

- iii) Estimate the α_k using average values for the n_k :

$$\hat{\alpha}_k = \frac{\bar{n}_k}{\sum_{i=1}^m \bar{n}_i} \quad (2.5)$$

where \bar{n}_k is the average number of events leading to the common cause failure of k components. If there are N modified impact vectors in the CCF event data base,

$$\bar{n}_k = \sum_{j=1}^N P_{kj} \quad (2.6)$$

This use of the average values for the n_k is approximate. Ref. 17 provides an exact approach for dealing with data uncertainties, but also shows that the error in the point estimate for α_k generated using Eq. (2.5) is usually small.

The application of this estimation procedure in the analysis of RHR pump

common cause failures is discussed in Section 2.3.

2.2 DEVELOPMENT OF SCREENED RHR PUMP FAILURE EVENT DATA BASE

This section discusses the collection of failure event data regarding RHR pumps (with an emphasis on common cause failures) and the screening of this data prior to application to the JAF RHR system. The screening is based on the rules provided in Section 2.1.3, the assumptions and boundary conditions of the RHR system model, and the plant-specific conditions at JAF. Also discussed are the root causes and the coupling mechanisms underlying each of the multiple failure events in the screened data base.

2.2.1 Data Sources

Ref. 18 provides an analysis of RHR pump failure events occurring over the period 1972 through 1981. Ref. 19 summarizes RHR pump failure events for the period 1972 through 1980. Ref. 19 provides more information on system performance and failure causes, and is used as the basis for the quantitative analysis done in this study.

2.2.2 Selection of Events

Ref. 19 provides one-line descriptions of pump failure events sorted by system. There are 76 RHR pump failure events included in this listing. Of these 76 events, 17 are found to be applicable. The screening process employs the following criteria:

- Pre-operational failure events are eliminated. (These events are identified by comparing the commercial operation date and the date of the event.)
- Most failure events coded as "loss of function" and "leakage/rupture" are eliminated. As stated in Ref. 19, "loss of function" refers to degraded performance of the pump, but the pump continues to run. Only those events in which the pump eventually stopped (or failed to start in the first place) are included.
- Failure events involving components outside of the pump boundary (as modeled in the PRA) are not included. The following components are considered to be within the pump boundary:
 - driver (the motor)
 - pump to motor coupling
 - other pump hardware, including casing, impeller, shaft, bearing
 - pump motor circuit breaker
 - pump motor control circuit, panel, switch, relay
- Pump failures caused by the failure of operators to restore the system following testing or maintenance are not included. [These are modeled as part of ϕ_{he} in Eq. (1.5)].
- Only "fail to start" events are included. Runtime failures, although observed, do not contribute significantly to plant risk.

Table 2.1 provides a listing of the 17 events surviving the screening process. Table 2.2 indicates the plant name, the population of RHR pumps at the plant, the number of RHR system demands, and the total run (exposure) time. Table 2.3 provides the failure codes used in Table 2.1.

2.2.3 RHR Pump Failure Mechanisms

Some understanding of the failure mechanisms underlying the RHR pump failure events in Table 2.1 is needed in order to develop the impact vectors for these events. This understanding is also essential to the assessment of the impact of various maintenance program changes on the likelihood of common cause failure.

Two particular issues are of interest: what was the failure root cause, and how did more than one component become susceptible to the same failure cause at the same time, i.e., what was the "coupling mechanism." With the identification of root causes and coupling mechanisms, the effectiveness of CCF defense tactics implicit in the current (or modified) maintenance practices at JAF can be evaluated.

A breakdown of the failure mechanisms for RHR pump ('Fail to Start' mode) is presented in Figure 2.1. This figure is based on the pump component boundary definition given in Section 2.2.2.. In principle, it would be desirable to study the maintenance impact for all the failure mechanisms identified in Figure 2.1. However, supporting data are sparse. We therefore focus our attention on the set of observed failure mechanisms as discussed below.

2.2.3.1 Root Causes

Knowledge of a failure event's root cause is important because it indicates how defenses can be constructed to prevent the causal chain of events that eventually led to failure. However, since defenses can be applied at different points in the chain, and since the concept of a root cause is generally tied to the defenses being considered,

different analysts may identify different "root causes" for the same event. In this work, root causes of failure events are defined in terms of the maintenance program. Events occurring after the root cause but before the final failure event are termed "proximate causes" by Ref. 13.

A "proximate cause" of a failure event is a condition that is readily identifiable as leading to the failure. For example, an event may involve a pump failure due to a failed motor; the motor failed because of a lack of lubrication. A proximate cause for the event is the lack of lubrication. However, the eventual cause of the lack of lubrication, as shown in Table 2.4, could be a deficiency in the maintenance program. If so, then this deficiency is the root cause of the event.

Ref. 13 provides two concepts useful for the systematic review of the failure event data, especially for the analysis of environment-caused failures. These are the notions of a "conditioning event" and a "trigger event." A "conditioning event" is an event that predisposes a component to failure or increases its susceptibility to failure, but does not of itself cause failure. In the previous example (failed pump motor), possible conditioning events are the failure of maintenance personnel to properly lubricate the motor moving parts and the lubrication oil quality does not meet required standards. (Note that the notion of an "event" is somewhat stretched by the last example.) The effect of the conditioning event is latent, but the conditioning event is, in this and other cases, a necessary contributor to the failure mechanism.

A "trigger event" is an event that activates a failure or initiates the transition to the failed state, regardless of whether that failure is revealed at the time the trigger event occurs. In the previous example, the trigger event is not indicated by the event description. A trigger event, particularly in the case of CCF events, is usually an event external to the components in the question.

The root causes for the 17 events listed in Table 2.1 are presented in Table 2.5. These are later used when assessing the CCF event impact vectors.

2.2.3.2 Coupling Mechanisms

In order for a multiple failure event to result from an initial root cause, the conditions have to be conducive to the trigger event and/or the conditioning events affecting all components simultaneously. (In this context, "simultaneous" failures are failures that occur close enough in time such that redundant components cannot perform their mission.) In other words, a "coupling mechanism" which links the failures of multiple equipment must exist.

More formally, a "coupling mechanism" (sometimes referred as coupling factor) is a characteristic of a group of component or piece parts that identifies them as susceptible to the same causal mechanisms of failure [12,13]. Three categories of coupling mechanisms for dependent failure events are functional, spatial, and human coupling mechanisms. For CCF analysis, the last two categories are the most applicable. Functional coupling of failures, such as the failure of a pump due to the failure of its supply bus, is usually treated explicitly in PRA system models. Spatially coupled failures involve situations where the failed components are exposed to the same environmental threat (e.g., high temperature). Human coupled failures can take many forms, including design errors, operation errors, maintenance errors, etc.

The coupling mechanisms for the 17 events listed in Table 2.1 are presented in Table 2.6. These are later used when assessing the CCF event impact vectors.

2.3 MODELING MAINTENANCE IMPACT ON CCF RATES

The approach for quantifying the effect of maintenance program changes on the α -factors is described in this section. This approach is outlined in Figure 2.2. The approach is applied to the JAF maintenance program and postulated changes in that program in Chapter 3.

2.3.1 Initial Impact Vectors for Actual Events

As stated in Section 2.1.4, the first step in the estimation of the α -factors is the assessment of the initial impact vectors for each of the events in the data base. For each event, the analyst must determine:

- Whether the event involves independent failures, a non-lethal shock, or a lethal shock. A non-lethal shock has the potential to fail all of the components in a common cause component group. A lethal shock fails all of the components in the group.
- The conditional failure probability ρ for a single component, given a non-lethal shock (if the event involves a non-lethal shock). This parameter is used by the "mapping up" and "mapping down" procedures described in Ref. 12, as discussed in Section 2.3.3.

If the number of components failed is less than the total number of components in the common cause component group, it can be expected that ρ is neither very small (close to 0) or very large (close to 1). The following assignment rules are used for ρ . Let m be the size of the common cause component group, and let k be the number of components actually failed

$$m = 2: \quad \rho = \begin{cases} 0.5 & \text{if } k = 1 \\ 0.8 & \text{if } k = 2 \end{cases}$$

$$m = 3: \quad \rho = \begin{cases} 0.3 & \text{if } k = 1 \\ 0.6 & \text{if } k = 2 \\ 0.8 & \text{if } k = 3 \end{cases}$$

$$m = 4: \quad \rho = \begin{cases} 0.2 & \text{if } k = 1 \\ 0.4 & \text{if } k = 2 \\ 0.6 & \text{if } k = 3 \\ 0.8 & \text{if } k = 4 \end{cases}$$

- The impact vectors for each event [see Eq. (2.3)]. In the case of independent events, separate impact vectors are created for each event. In the case of lethal shocks, $q_{kj} = 0.0$ for $k \neq m$ and $q_{mj} = 1.0$. In the case of non-lethal shocks, judgment based on the qualitative event description (which allows an inference of the underlying coupling mechanism) is employed.

The impact vectors for the 17 events listed in Table 2.1 are presented in Table 2.7.

2.3.2 Degree of Applicability to JAF

The second step in the estimation process, following the creation of the impact vectors for the actually experienced CCF events (the initial impact vectors), is the creation of impact vectors relevant to the plant being analyzed (the modified impact vectors). This second step employs an assessment of the degree of applicability of each CCF event to the plant being analyzed, a mapping of the initial impact vectors to the modified impact vectors (if the sizes of the common cause component groups at the plants are different), and an assessment of the degree to which the modified impact vector profiles (the relative values of the p_k) are different from the initial

impact vector profiles (the relative values of the q_k). This section discusses the applicability assessment. The applicability assessment procedure described below is illustrated in Figure 2.3. The mapping up/down procedure is briefly discussed in Section 2.3.3. The assessment of changes in impact vector profiles is not performed in this study; it is judged that such changes represent second order effects in the estimation of α -factors.

When analyzing the applicability of a CCF event, the following question must be answered: Given all the qualitative differences between the two plants/systems, to what extent are the root cause(s) and coupling mechanism(s) observed in the event relevant to the system being analyzed (the "new" system)? Clearly, judgment must be employed to answer this question. The following sections describe a procedure that is useful in structuring this judgment. When applied to a given event in the screened CCF event data base, the procedure results in two values for the probabilities that the event's root causes and coupling mechanisms are applicable to the plant being analyzed. These probabilities are termed the "root causes applicability" and the "coupling mechanisms applicability" of the event.

The following discussion presents the model used to integrate these applicabilities into the α -factor estimation process. Two kind of events are treated: 1) single failure events for which only root causes have been identified, and 2) multiple failure events for which both root causes and coupling mechanisms have been identified.

Denote the root cause applicability of Event j by app_rc_j , and the coupling mechanism applicability of Event j by app_cm_j .

The average impact vector for Event j when Event j involves multiple failures is then obtained as follows:

$$\begin{aligned}
p_j &= (app_rc_j * app_cm_j) * q_j (\text{given that Event } j \text{ is applicable}) \\
&\quad + (1 - app_rc_j * app_cm_j) * q_j (\text{given that Event } j \text{ is not applicable}) \\
&= (app_rc_j * app_cm_j) * q_j (\text{given that Event } j \text{ is applicable})
\end{aligned}
\tag{2.7}$$

The average impact vector for Event i when Event i involves only a single failure is obtained as follows:

$$\begin{aligned}
p_i &= app_rc_i * q_i (\text{given that Event } i \text{ is applicable}) \\
&\quad + (1 - app_rc_i) * q_i (\text{given that Event } i \text{ is not applicable}) \\
&= app_rc_i * q_i (\text{given that Event } i \text{ is applicable})
\end{aligned}
\tag{2.8}$$

It can be seen that the single failure analysis and the multiple failure analyses are similar; the effective applicability is:

$$app = \begin{cases} app_rc_j * app_cm_j & \text{for multiple failure event;} \\ app_rc_i & \text{for single failure event;} \end{cases}
\tag{2.9}$$

As an example, consider Event 9 in Table 2.1. The plant experiencing this event (Dresden 2) has 3 RHR pumps. The original impact vector assessed for Event 9 is

$$q_9 = (0, 0.8, 0.1, 0.1)$$

If the assessed root causes applicability is app_rc_9 , and coupling mechanisms applicability is app_cm_9 , then from Eq. (2.9), we have

$$app_0 = app_rc_0 * app_cm_0$$

If the plant being analyzed also has 3 RHR pumps, the modified impact vector suitable for use in estimating α_k ($k = 1$ to 3) is:

$$p_0 = (1 - app_0, 0.8 * \alpha\rho_0, 0.2 * \alpha\rho_0, 0, 0) \quad (2.10)$$

If the plant being analyzed has more or less than 3 RHR pumps, this impact vector must be modified using the "mapping down" or "mapping down" procedures described in Ref. 12. The mapping process for this sample event is discussed in the next section.

The applicabilities (app_rc and app_cm) of a CCF event are functions of the event's root cause(s) and coupling mechanism(s), and of the analyzed plant's defenses with respect to these root cause(s) and coupling mechanism(s). The root causes and coupling mechanisms for the CCF events are shown in Tables 2.5 and 2.6.

The quantitative effects of the root cause defenses, i.e., actual maintenance practices conducted in the plant, are determined using Table 2.8. This table is called the "root cause-maintenance defense matrix" (RC-MD matrix). The row headings in this matrix represent possible root causes; the column headings represent the possible (maintenance-program level) defenses against conditioning events that will allow the root cause to propagate to a failure. By providing more maintenance program defenses, the likelihood of the root cause propagating to a failure is reduced (strengthening a given defense reduces the likelihood that a conditioning event occurs). The entries in the matrix indicate which of the following tables (Tables 2.9-2.12) should be used in the root cause portion of the

applicability analysis; their use is described below. The entries in Tables 2.9–2.12 are based on failure rate multipliers collected from Ref. 13 . It is assumed that these failure rate multipliers can be used directly in an applicability assessment.

The quantitative effects of the coupling mechanism defenses are determined using Table 2.13. This table is called the "coupling mechanism–maintenance defense matrix" (CM–MD matrix). The row headings in this matrix represent possible coupling mechanisms; the column headings represent the the possible (maintenance–program level) defenses against conditioning events that will allow the coupling mechanism to link multiple failures. The entries in the matrix indicate which of Tables 2.14–2.17 should be used in the coupling mechanism portion of the applicability analysis; their use is described below. The entries in Tables 2.14–2.17 are also based on failure rate multipliers Ref. 13. It is assumed that these failure rate multipliers can be used directly in an applicability assessment.

To following procedure quantifies the applicabilities, *app_rc* and *app_cm*, of a particular CCF event.

Step 1

General: Use the original impact vector to obtain the base root cause weight and the base coupling mechanism weight. The former is the value of q_{1j} ; the latter is the sum of the q_{kj} for which $k > 1$.

Example: Continuing the example with Event 9, the base root cause weight is the probability that the event involved only a single pump failure. As seen in Table 2.7, this has a value of 0.8. The base coupling mechanism weight is the probability that the event involved multiple pump failures.

Table 2.7 shows that this has a value of 0.2.

Step 2

General: Distribute the base root cause weight between identified root causes using distribution factors for each root cause–maintenance defense (RC–MD) combination. In principle, several root causes can contribute to a single failure event. The assessed distribution of root cause weight is used in Step 4 below.

Assuming that one of the root causes is dominant, the following three rules are used to assign distribution values for each RC–MD combination:

- Two contributing root causes: the dominant root cause is assigned a distribution factor of 0.8; the other root cause is assigned a distribution factor of 0.2.
- Three contributing root causes: the dominant root cause is assigned a distribution factor of 0.6; the other root causes are assigned distribution factor of 0.2 each.
- Four contributing root causes: the dominant root cause is assigned a distribution factor of 0.7; the other root causes are assigned distribution factor of 0.1 each.

Note that if more maintenance defenses are included in Table 2.8, these rules may need to be extended. For this study, since no more than 4 root causes ever appear in a event, the rule stops at the level of 4

contributors.

Example: Assume that two root causes for Event 9 are the lack of RHR pump-specific training and the complete reliance on corrective maintenance. Let the latter be the dominant one. Then the root cause distribution factors (one for each RC-MD combination) are:

$$D_Factor_{rc-md}(CM) = 0.8$$

$$D_Factor_{rc-md}(\text{No Training}) = 0.2$$

Step 3

General: Distribute the base coupling mechanism weights between each coupling mechanism-maintenance defense (CM-MD) combination. This is done in the same manner (and with the same rules) as for the root cause weights.

Example: For Event 9, assume that the coupling mechanisms involve the use of deficient procedures for maintenance, and the same maintenance crew for both pumps without staggered maintenance. Assuming that the latter is dominant, we have:

$$D_Factor_{cm-md}(\text{Deficient_Procedure}) = 0.2$$

$$D_Factor_{cm-md}(\text{Staff_Scheduling}) = 0.8$$

Step 4

General: For each contributing root cause and maintenance defense, assess the appropriate RC–MD multiplier (this is a function of the current maintenance practice). This multiplier is the ratio of: a failure rate multiplier specific to the plant being analyzed, and a failure rate multiplier specific to the plant actually experiencing the CCF event. Thus, it measures the relative difference between the maintenance practices of the two plants with respect to the root cause/maintenance defense combination. If the maintenance practices at the plant experiencing the CCF event are unknown, an average multiplier is used in the denominator of the ratio.

Compute the weighted sum of these RC–MD multipliers, where the weights are obtained in Step 2 above. This weighted sum is denoted as *app_rc*, the applicability of the root causes.

Perform a similar task for each contributing coupling mechanism, to obtain the weighted sum of the CM–MD multipliers. The weights are obtained in Step 3 above. This weighted sum is denoted as *app_cm*, the applicability of the coupling mechanisms.

The product of *app_rc* and *app_cm* is the total applicability for the event.

Example: Assume that at the plant being analyzed, the maintenance crew is trained in the procedures specific to the RHR pumps. The relevant entry in Table 2.8 is 'm2'; this indicates that Table 2.10 is used to

provide the multiplier value.

$$\text{Multiplier}_{rc-md}(\text{Training}) = \frac{0.95}{1.20} = 0.79$$

Assume that at the plant being analyzed, only the corrective maintenance is used. The relevant entry in Table 2.8 is 'm3'; this indicates that Table 2.9 is used to provide the multiplier value.

$$\text{Multiplier}_{rc-md}(\text{CM}) = \frac{1.4}{1.4} = 1$$

The total applicability rating for the contributing root causes is then given by

$$\begin{aligned} app_rc_9 = & D_Factor_{rc-md}(\text{CM}) * \text{Multiplier}_{rc-md}(\text{CM}) + \\ & D_Factor_{rc-md}(\text{No Training}) * \text{Multiplier}_{rc-md}(\text{Training}) \end{aligned} \quad (2.11)$$

$$app_rc_9 = 0.8 * 1 + 0.2 * 0.79 = 0.958$$

The total applicability rating for the contributing coupling mechanisms is found in a similar manner. Assuming that, at the plant being analyzed, the same staff personnel are used to perform maintenance on two loops, but the maintenance is staggered. The relevant entries in Table 2.13 are 'm5' and 'm6'. The entry in Table 2.13 corresponding to the deficient quality of procedures is 'm8'.

$$\text{Multiplier}_{\text{cm-md}}(\text{Staff_Scheduling}) = \frac{0.5}{1} * \frac{0.2}{0.2} = 0.5$$

$$\text{Multiplier}_{\text{cm-md}}(\text{Deficient_Procedure}) = \frac{0.5}{0.5} = 1$$

Thus

$$\begin{aligned} \text{app_cm}_9 = & \text{D_Factor}(\text{Staff_Scheduling}) * \\ & \text{Multiplier}_{\text{cm-md}}(\text{Staff_Scheduling}) + \\ & \text{D_Factor}(\text{Deficient_Procedure}) * \\ & \text{Multiplier}_{\text{cm-md}}(\text{Deficient_Procedure}) \end{aligned} \quad (2.12)$$

$$\text{app_cm}_9 = 0.8*0.5 + 0.2*1 = 0.6$$

Thus the effective applicability is

$$\text{app}_9 = \text{app_rc}_9 * \text{app_cm}_9 = 0.57$$

Thus the intermediate impact vector of Event 9 to be used in estimating the *a*-factors for the plant being analyzed is, using Eq. (2.10)

$$\mathbf{p}_9 = (0.43, 0.46, 0.06, 0.6)$$

This intermediate impact vector needs to be modified to account for possible differences in system size (between the plant being analyzed and the plant experiencing the event). The mapping up/down procedures used to accomplish this are described briefly in the following section.

The example calculation provided in this section applies to a single plant's maintenance program. It can be seen that the same approach can be used to determine the impact of maintenance programs changes on event applicability.

2.3.3 Mapping Up and Mapping Down

The applicability analysis is used to determine the degree to which a CCF event in the data base is applicable to the plant being analyzed. Even after the applicability analysis is performed, however, some adjustments to the impact vector may be required to account for differences in system size.

To account for differences in system (or more precisely, common cause component group) size, Ref. 12 provides "mapping up" and "mapping down" procedures. These procedures are summarized in Tables 2.18 and 2.19; it can be seen that the parameter ρ assessed earlier in Section 2.3.1 is needed at this point.

Continue with Event 9. For the JAF plant being analyzed, the RHR system has 4 pumps (i.e., $m = 4$). This is different from the size of the Dresden 2 RHR system which experiences Event 9. Thus, a mapping up calculation is needed to account for this difference.

From Table 2.7, we assess the shock failure probability of Event 9 to be 0.5. Using the equations in Table 2.18 for 3 \rightarrow 4 mapping, we have the following final impact vector for Event 9:

$$p_9 = (0.425, 0.429, 0.178, 0.058, 0.017)$$

This applies to the JAF plant design and current JAF maintenance practices.

Using the above procedure, the final impact vectors for all 17 RHR pump failures, modified to account for applicability and system size, are developed. These are presented in Table 2.20. These are used in the estimation of the α -factor model parameters, as described in the following section.

2.3.4 Estimation of CCF Parameters

Given the impact vectors in Table 2.20, the α -factors can be estimated in a

straightforward fashion using Eqs. (2.5) and (2.6). Note that the data provided by Ref. 19 are also useful for estimating ϕ_d , the total demand failure rate at the system of the plant being analyzed. For the baseline case analyzed in this chapter, we have

$$\hat{\phi}_d = \frac{1}{4N_d} \sum_{k=1}^4 k \cdot \bar{n}_k \quad (2.13)$$

In Chapter 3, modified demand failure rates, $\hat{\phi}_d'$ are calculated using the failure rate modifiers defined in Table 2.8 – Table 2.17. The $\hat{\phi}_d$ from the baseline case is used as a base value in the calculations. The equation used for the calculation of ϕ_d' is:

$$\begin{aligned} \phi_d' = \hat{\phi}_d * \prod_{i=1..4} \left[\frac{M_{rc-md-i} \text{ (Current maintenance level)}}{M_{rc-md-i} \text{ (Baseline case level)}} \right] \\ * \prod_{j=5..8} \left[\frac{M_{cm-md-j} \text{ (Current maintenance level)}}{M_{cm-md-j} \text{ (Baseline case level)}} \right] \end{aligned} \quad (2.14)$$

The following maximum-likelihood estimates for the α -factor model parameters are obtained using the root cause and coupling mechanism distribution factors/multipliers that best characterize the JAF maintenance program:

$$\begin{aligned} \hat{\alpha}_1 &= 0.76 \\ \hat{\alpha}_2 &= 0.18 \\ \hat{\alpha}_3 &= 0.05 \\ \hat{\alpha}_4 &= 0.01 \\ \hat{\phi}_d &= 0.005 \end{aligned}$$

Using Eq. (2.1), point estimates for Q_k are found:

$$\hat{Q}_1 = 0.003$$

$$\hat{Q}_2 = 4.7 \cdot 10^{-4}$$

$$\hat{Q}_3 = 1.9 \cdot 10^{-4}$$

$$\hat{Q}_4 = 1.6 \cdot 10^{-4}$$

Table 2.1 - 17 Events Surviving Screening (Page 1 of 2)

No.	Plant Name	Event Date	Failure Code, Type, Class;	Failure Mode	Failure Cause
1	DB1	011678	B13, T, T	Decay heat pump 1-1; Fuses in BKR. Start CKT	Poor fuse contact in CKT
2	DB1	110679	B13, T, T	DHR pump 1 failed to start	Faulty switch
3	BR1	060177	B13, S, D	1A RHR did not start on auto-signal	Sticky contactor on control switch
4	BR1	110577	B02, S, T	RHR 1A did not start; cover loose and contact corroded	Corroded due to water leaks
5	BR1	010979	B13, S, D	RHR pump 'D' would not start	Internal problems in circuit breaker
6	BR2	040479	B13, U, T	RHR pumps 2B and 2D Would not start from RTGB	Poor connections on fuses and fuse box
7	CO1	122379	B13, S, D	RHR pump '1D' would not operate	Breaker failure
8	DA1	042375	B13, S, D	RHR pump 229B failed to start	Logic relay E11-k708 did not trip as required
9	DR2	062576	B19, T, D	2C LPCI failed to start from maintaining tours WTR. TEMP.	Dirty switch in 4kv for pump
10	DR2	041579	B00, , U	2A LPCI pump would not start	Cause unknown

Table 2.1 - 17 Events Surviving Screening (Page 2 of 2)

No.	Plant Name	Event Date	Failure Code, Type, Class;	Failure Mode	Failure Cause
11	EN1	070175	B13, S, D	RHR 1B air circuit breaker failed to close	Slipped cam in latch assemb. of ACB
12	EN2	041580	B13, S, D	'D' RHR pump failed to start on LOCA signal	Wire missing from terminal No.7 on relay
13	FP1	121274	B18, S, D	RHR pump 10P-3D failed to start; replaced faulty BKR	breaker DC charging motor burned out
14	FP1	102079	B13, S, T	RHR pump 'C' failed to start properly	Limit switch not adjusted properly
15	PB2	042978	B01 S, D	Unit 2 'B' and 'D' RHR pumps blocked for 2 hours	Operator removed unit 2 instead of unit 3 pump
16	VY1	011877	B13, S, D	'D' RHR pump would not start	A loose lead in a breaker caused failure
17	TR1	052577	B13, T, D	B RHR Pump did not start- Automatic	Sequencer contacts open with too low CRNT

**Table 2.2 – Population Data for RHR Pump CCF Events
(Fail to Start)**

Plant Code	Plant Name	RHR Pump Population	Number of Demand	Total Run Time(hrs)
DB1	Davis–Besse 1	2	36	6521
BR1	Brunswick 1	4	48	11223
BR2	Brunswick 2	4	65	13558
CO1	Cooper Station	4	78	22750
DA1	Duane Arnold	4	77	17591
DR2	Dresden 2	3	105	29346
EN1	Edwin I. Hatch 1	4	73	19553
EN2	Edwin I. Hatch 2	4	27	5074
FP1	J.A. Fitzpatrick	4	70	15390
PB2	Peach Bottom 2	4	85	20249
VY1	Vermont Yankee	4	102	28713

Table 2.3 – Failure Codes Used in Table 2.1

Failure Code

<u>Failure Mode</u>		<u>Failure Cause</u>	
CODE	DESCRIPTION	CODE	DESCRIPTION
A	leakage / rupture	00	unknown
B	does not start	01	personnel (operations)
C	lose of function	02	personnel (maintenance)
D	does not continue run	03	personnel (testing)
		04	design errors
		05	fab./ construction/q-c
		06	procedural discrepancies
		07	normal wear
		08	excessive wear
		09	foreign material contamination
		10	corrosion / erosion
		11	extreme environment
		12	loose fastener
		13	elec./mech. control malfunction
		14	failed internal
		15	shaft / coupling failure
		16	loss of pressure boundary integrity
		17	improper clearances
		18	drive train failure
		19	seal / packing failure
		20	misalignment
		21	bearing failure

Type of Event

Event Classification

CODE DESCRIPTION

CODE DESCRIPTION

- B — recurring common cause failures
- C — common cause failures
- R — recurring failures
- S — command faults
- T — recurring command faults
- U — common cause command faults
- V — recurring common cause command faults

- D — demand
- T — time
- U — unknown

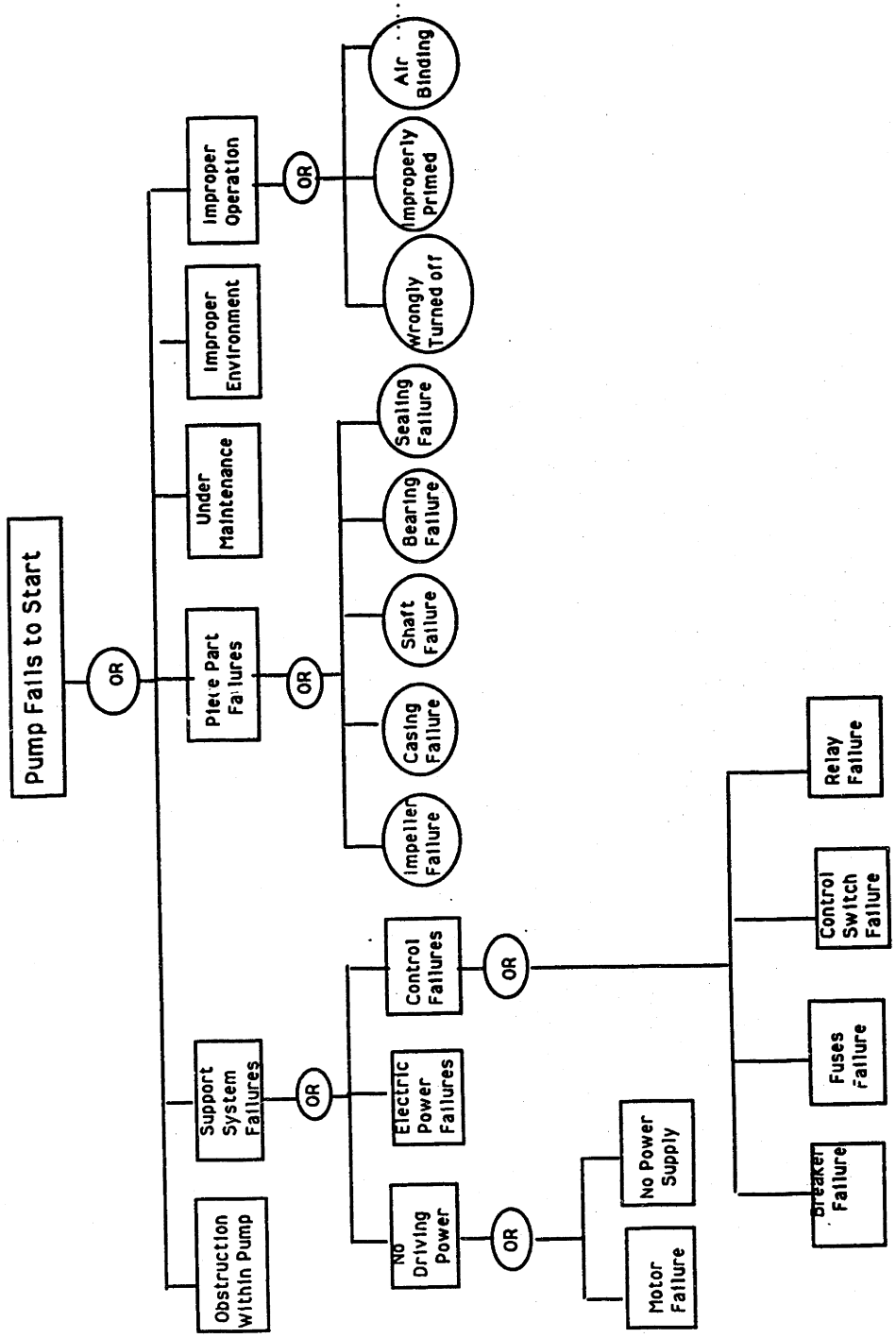


Figure 2.1: RHR Pump 'FS' Mode Failure Mechanisms

Table 2.4

**Example Cause–Effect Analysis of CCF event in original Event Data Base
(Lack of Lubrication)**

Immediate Cause/Reason	Effect/Problem
Motor Burst into flames	Pump fails to continue to run
Insufficient lubrication to LWR RAD. BRNG.	Motor burst into flames
Failure to perform preventive maintenance	Insufficient lubrication to LWR RAD. BRNG.
Foreman did not remember to do it	Failure to perform preventive
Foreman did not perform the job properly	Failure to perform preventive maintenance
Programmatic deficiency: there is no formal scheduling system to plant preventive maintenance activities; or procedure has not 2nd checking	Foreman did not remember to do it
There is no training provided on lubrication job	Foreman did not perform the job properly

Table 2.5 - Root Cause for RHR Pump CCF Events

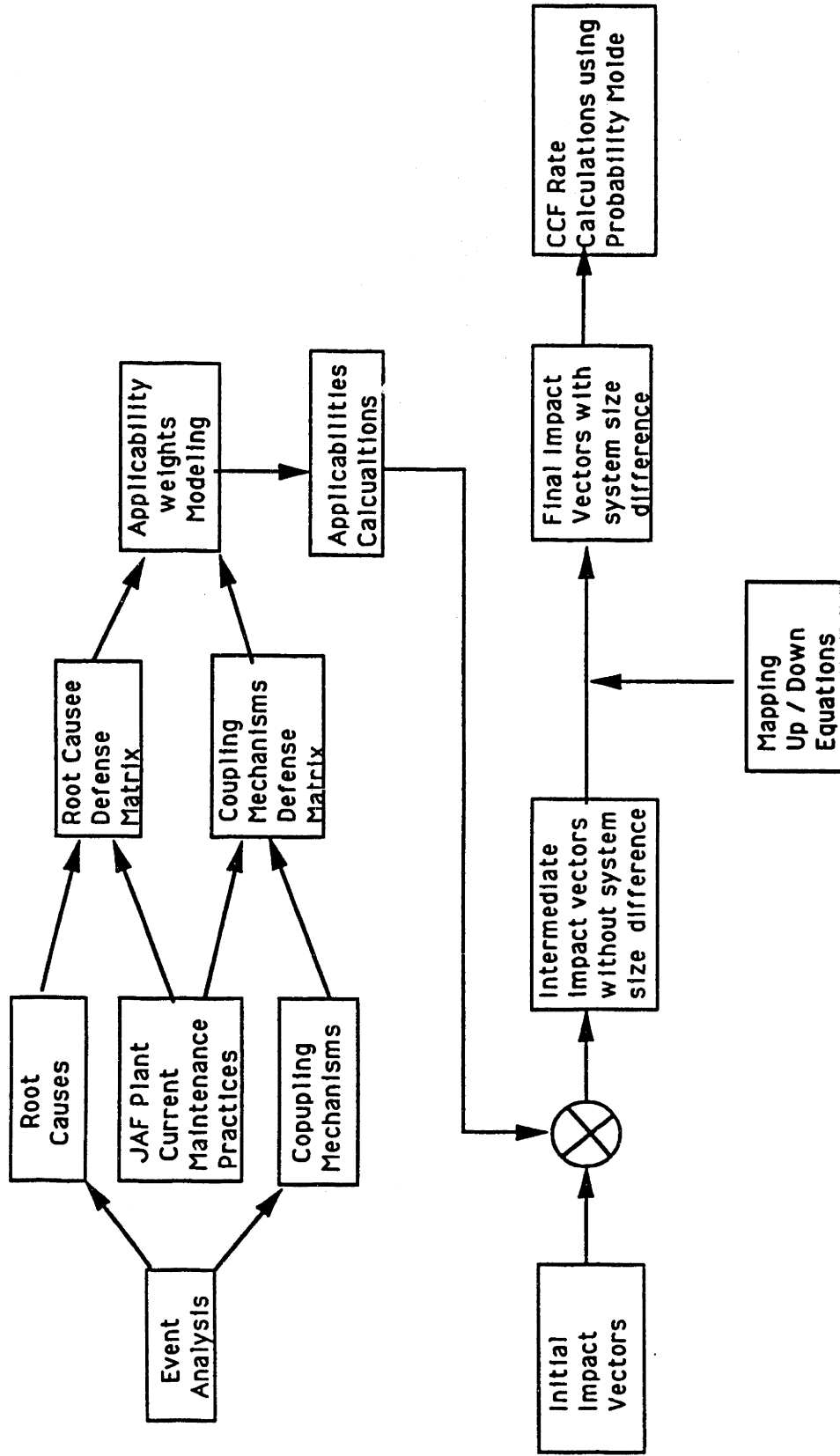
Event Number	Plant Name	Conditioning Event	Root Causes (MP Blocks related)
1	DB1	Fuses poorly connected	Procedure bad; personnel not trained; only CM (d)
2	DB1	Control switch internal failure	Only corrective maintenance (d); No training on personnel
3	BR1	Enviro. contamin. on control switch	Only corrective maintenance (d); No training on personnel
4	BR1	Pump cover corroded due to leaking	Only corrective maintenance (d); no training
5	BR1	Circuit breaker internal failure	Procedure bad; personnel not trained; only CM (d)
6	BR2	Fuse poorly conneted	Procedure bad; personnel not trained; only CM (d)
7	CO1	Circuit breaker internal failure	Procedure bad; personnel not trained; only CM (d)
8	DA1	Relay internal failure	Procedure bad; personnel not trained; only CM (d)
9	DR2	Enviro. contamin. on control switch	Only corrective maintenance (d); No training on personnel
10	DR2	No obvious evidence observed	All three possible root causes a in No.1
11	EN1	Circuit breaker internal failure	Procedure bad; personnel not trained; only CM (d)
12	EN2	Relay wire missing	Procedure bad; Personnel not trined(d)
13	FP1	Circuit breaker internal failure	Only corrective maintenance (d); No training on personnel
14	FP1	Control switch disabled by human error	Procedure bad; personnel not trained (d)
15	PB2	Pump disabled by human error	Procedure bad; personnel not trained (d)
16	VY1	Circuit breaker poorly connected	Procedure bad; personnel not trained; only CM (d)
17	TR1	Sequencial contact open due to low CRNT	Procedure bad; Only corective maintenance (d)

Note: (d) means dominant

Table 2.6 - Coupling Mechanisms for RHR Pump CCF Events

Event Number	Plant Name	Conditioning Event	Coupling Mechanisms(MP block related)
1	DB1	Fuses poorly connected	
2	DB1	Control switch internal failure	Staff scheduling (d); Same deficient procedure used
3	BR1	Enviro. contamin. on control switch	
4	BR1	Pump cover corroded due to leaking	Staff scheduling (d); Same deficient procedure used
5	BR1	Circuit breaker internal failure	
6	BR2	Fuse poorly connected	Staff scheduling (d); Same deficient procedure used
7	CO1	Circuit breaker internal failure	
8	DA1	Relay internal failure	
9	DR2	Enviro. contamin. on control switch	Staff scheduling(d); Same Deficient procedure;
10	DR2	No obvious evidence observed	
11	EN1	Circuit breaker internal failure	
12	EN2	Relay wire missing	
13	FP1	Circuit breaker internal failure	
14	FP1	Control switch disabled by human error	Staff scheduling (d); same deficient procedure;
15	PB2	Pump disabled by human error	Staff scheduling (d); same deficient procedure;
16	VY1	Circuit breaker poorly connected	
17	TR1	Sequential contact open due to low CRNT	Deficient Procedure used(d)

Note: (d) means dominant



Note: \otimes means multiplication.

Figure 2.2 - Approach For Quantifying CCF Parameters

Table 2.7 - Initial Impact Vectors for RHR Pump CCF Events (Fail to Start)

Event Number	Plant Name	P0	P1	P2	P3	P4	Shock Type	Shock Failure Probability p
1	DB1	{ 0	1	0 }			I	
2	DB1	{ 0	1	0 }			NL	0.5
3	BR1	{ 0	1	0	0	0 }	I	
4	BR1	{ 0	0.8	0.2	0	0 }	NL	0.4
5	BR1	{ 0.9	0.1	0	0	0 }	I	
6	BR2	{ 0.7	0	0.2	0	0.1 }	NL	0.2
7	CO1	{ 0.9	0.1	0	0	0 }	I	
8	DA1	{ 0	1	0	0	0 }	I	
9	DR2	{ 0	0.8	0.1	0.1 }		NL	0.3
10	DR2	{ 0.8	0.2	0	0 }		I	
11	EN1	{ 0	1	0	0	0 }	I	
12	EN2	{ 0	1	0	0	0 }	I	
13	FP1	{ 0	1	0	0	0 }	I	
14	FP1	{ 0	0.7	0.1	0.1	0.1 }	NL	0.2
15	PB2	{ 0	0	1	0	0 }	NL	0.2
16	VY1	{ 0.9	0.1	0	0	0 }	I	
17	TR1	{ 0	1	0 }			NL	0.5

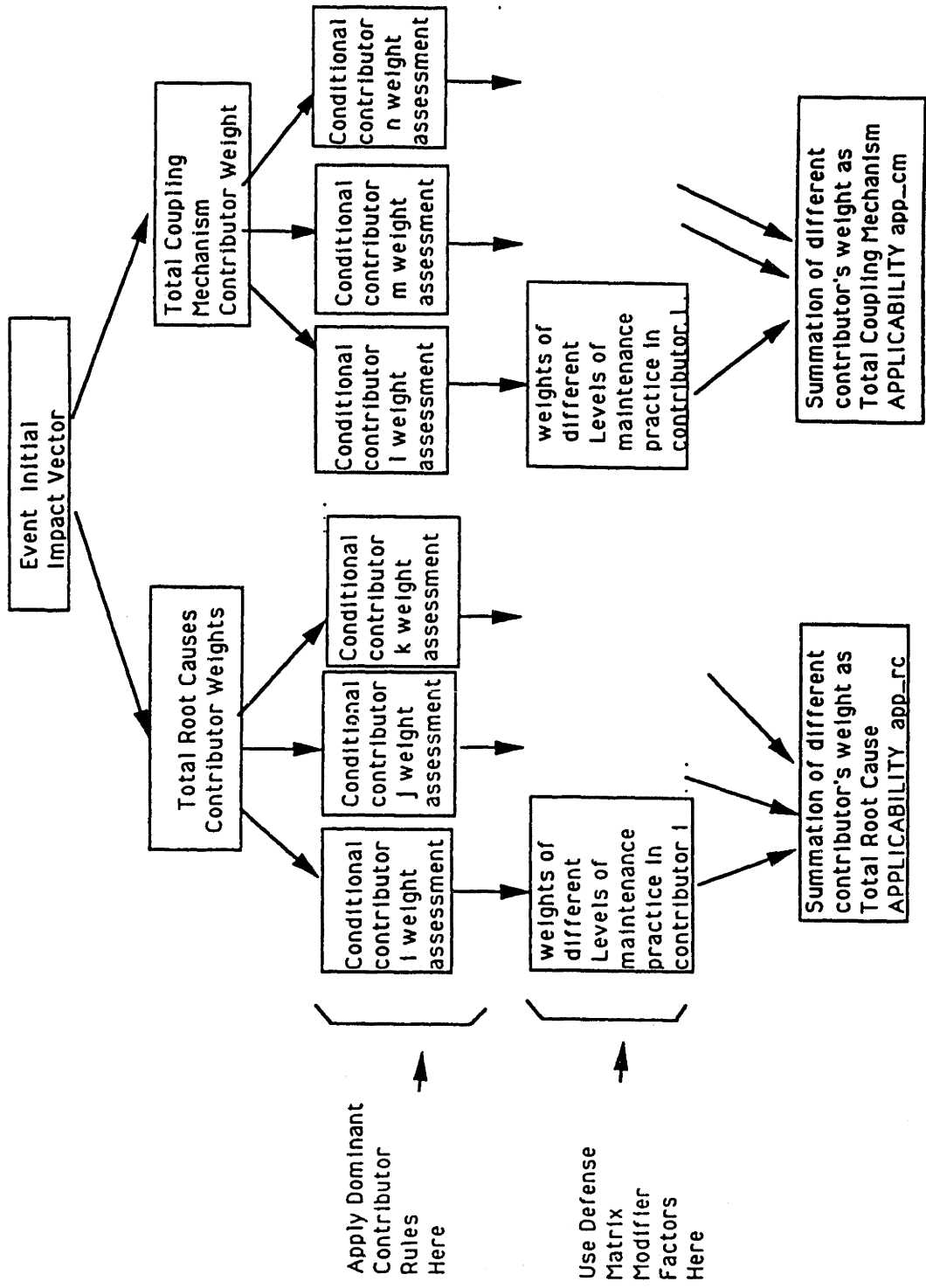


Figure 2.3 - Approach for Quantifying CCF Event - Applicability -

Table 2.8 Root Cause - Maintenance Defense Matrix

Conditioning Events	Selected Defense Against the Root Causes									
	BLOCK 1			BLOCK 2	BLOCK 8		BLOCK 9			
	Maintenance Scheduling	Staff Assignment	Shift Coverage	Quality of Maintenance	Quality of Training	Training Levels	Quality of Procedures			
Fuses with Poor Connection				m1	m2	m3				
Wrong Circuit Breaker Is Installed						m3	m4			
Breaker Internal Failures				m1	m2	m3				
Breaker with Poor Connection				m1	m2	m3				
Environmental Contamination On Breakers				m1	m2	m3				
Control Switch Disabled by Human Error						m3	m4			
Control Switch Internal Failures				m1	m2	m3				
Environmental Contamination On Control Switch				m1	m2	m3				
Relay Internal Failure				m1	m2	m3				
Pump Disabled by Human Errors						m3	m4			

Note: The empty entries means that no defense are available. Qualitatively, they mean that those modifiers are equal to one.

Table 2.9 – Multipliers for Factor ' m1 '

Quality of Maintenance	Failure Rate Modifier *			
	Fuses	Breakers	Control Switches	Relay
Predictive	0.88	0.91	0.89	0.95
Preventive	1.15	1.1	1.2	1.1
Corrective	1.4	1.3	1.67	1.5

*: The modifier provided in ANSI/IEEE Std 493-1980 is to multiply the total equipment failure rate.

Table 2.10 – Multipliers for Factor ' m2 '

Quality of Training	Failure Rate Modifier	
	Electrical/Machanical Component	
Trained in Specific Procedure	0.95	
Not trained on specific procedure	1.2	

Table 2.11 – Multipliers for Factor ' m3 '

Level of Training	Failure Rate Modifier	
	Electrical/Mechanical Component	
Corrective Level	1.3	
Preventive Level	0.9	
Predictive Level	0.75	

Table 2.12 – Multipliers for Factor ' m4 '

Procedure Quality	Failure Rate Modifier	
	Operation Actions	Maintenance/Surveillance/Testing Action
Procedure not used	1.6	1.5
Used, need Improvement	1.3	1.2
Used, good quality	0.9	0.8

Table 2.13: Coupling Mechanisms - Maintenance Defense Matrix

Failure Mechanisms	Selected Defense Against the Conditioning Events								
	BLOCK 1			BLOCK 2	BLOCK 8		BLOCK 9		
	Maintenance Scheduling	Staff Assignment	Shift Coverage	Quality of Maintenance	Quality of Training	Training Levels	Quality of Procedures		
Fuses with Poor Connection	m5	m6					m8		
Wrong Circuit Breaker Is Installed	m5	m6	m7				m8		
Breaker Internal Failures	m5	m6					m8		
Breaker with Poor Connection	m5	m6					m8		
Environmental Contamination On Breakers	m5	m6					m8		
Control Switch Disabled by Human Error	m5	m6	m7				m8		
Control Switch Internal Failures	m5	m6					m8		
Environmental Contamination On Control Switch	m5	m6					m8		
Relay Internal Failure	m5	m6					m8		
Pump Disabled by Human Errors	m5	m6	m7				m8		

Note: The empty entries means that no defense are available. Qualitatively they means that these modifiers are equal to 1.

Table 2.14 – Multipliers for Factor ' m5 '

Maintenance Scheduling	Coupling Mechanisms Modifier
	All Components
Staggered on Trains	0.25
Staggered on Loops	0.5
Non Staggered	1

Table 2.15 – Multipliers for Factor ' m6 '

Staff Diversity	Coupling Mechanisms Modifier
	All Components
Different in Each Train	0.05
Different in Each Loop	0.1
Diversity not Implemented	0.2

Table 2.16 – Multipliers For Factor ' m7 '

Staff Area Allocations	Coupling Factor Modifier
	All components
Specific Area Specific Component	0.1
Whole Area Specific Component	0.2

Table 2.17 – Multipliers For Factor ' m8 '

Procedure Quality	Coupling Mechanism Modifier	
	Operation Actions	Maintenance/Surveillance/Testing Action
Procedure not used	1	1
Used, need improvement	0.6	0.5
Used, good quality	0.3	0.25

**Table 2.18 – Mapping Up Procedure
(from NUREG/CR-4780, Vol. 2, p. D-16)**

		SIZE OF SYSTEM MAPPING TO		
		2	3	4
SIZE OF SYSTEM MAPPING FROM	1	$P_1(2) = 2(1 - \rho)P_1(1)$ $P_2(2) = \rho P_1(1)$	$P_1(3) = 3(1 - \rho)^2 P_1(1)$ $P_2(3) = 3\rho(1 - \rho)P_1(1)$ $P_3(3) = \rho^2 P_1(1)$	$P_1(4) = 4(1 - \rho)^3 P_1(1)$ $P_2(4) = 6\rho(1 - \rho)^2 P_1(1)$ $P_3(4) = 4\rho^2(1 - \rho)P_1(1)$ $P_4(4) = \rho^3 P_1(1)$
	2		$P_1(3) = (3/2)(1 - \rho)P_1(2)$ $P_2(3) = \rho P_1(2) + (1 - \rho)P_2(2)$ $P_3(3) = \rho P_2(2)$	$P_1(4) = 2(1 - \rho)^2 P_1(2)$ $P_2(4) = (5/2)\rho(1 - \rho)P_1(2) + (1 - \rho)^2 P_2(2)$ $P_3(4) = \rho^2 P_1(2) + 2\rho(1 - \rho)P_2(2)$ $P_4(4) = \rho^2 P_2(2)$
	3			$P_1(4) = (4/3)(1 - \rho)P_1(3)$ $P_2(4) = \rho P_1(3) + (1 - \rho)P_2(3)$ $P_3(4) = \rho P_2(3) + (1 - \rho)P_3(3)$ $P_4(4) = \rho P_3(3)$

**Table 2.19 – Mapping Down Procedure
(from NUREG/CR-4780, Vol. 2, p. D-9)**

		SIZE OF SYSTEM MAPPING TO (NUMBER OF IDENTICAL TRAINS)		
		3	2	1
SIZE OF SYSTEM MAPPING FROM	4	$P_0^{(3)} = \frac{1}{4} P_1^{(4)} + P_0^{(4)*}$ $P_1^{(3)} = \frac{3}{4} P_1^{(4)} + \frac{1}{2} P_2^{(4)}$ $P_2^{(3)} = \frac{1}{2} P_2^{(4)} + \frac{3}{4} P_3^{(4)}$ $P_3^{(3)} = \frac{1}{4} P_3^{(4)} + P_4^{(4)}$	$P_0^{(2)} = \frac{1}{2} P_1^{(4)} + \frac{1}{6} P_2^{(4)}$ $P_1^{(2)} = \frac{1}{2} P_1^{(4)} + \frac{2}{3} P_2^{(4)} + \frac{1}{2} P_3^{(4)}$ $P_2^{(2)} = \frac{1}{6} P_2^{(4)} + \frac{1}{2} P_3^{(4)} + P_4^{(4)}$	$P_0^{(1)} = \frac{3}{4} P_1^{(4)} + \frac{1}{2} P_2^{(4)} + \frac{1}{4} P_3^{(4)}$ $P_1^{(1)} = \frac{1}{4} P_1^{(4)} + \frac{1}{2} P_2^{(4)} + \frac{3}{4} P_3^{(4)} + P_4^{(4)}$
	3		$P_0^{(2)} = P_0^{(3)} + \frac{1}{3} P_1^{(3)}$ $P_1^{(2)} = \frac{2}{3} P_1^{(3)} + \frac{2}{3} P_2^{(3)}$ $P_2^{(2)} = \frac{1}{3} P_2^{(3)} + P_3^{(3)}$	$P_0^{(1)} = P_0^{(3)} + \frac{2}{3} P_1^{(3)} + \frac{1}{3} P_2^{(3)}$ $P_1^{(1)} = \frac{1}{3} P_1^{(3)} + \frac{2}{3} P_2^{(3)} + P_3^{(3)}$
	2			$P_0^{(1)} = P_0^{(2)} + \frac{1}{2} P_1^{(2)}$ $P_1^{(1)} = \frac{1}{2} P_1^{(2)} + P_2^{(2)}$

*THE TERM $P_0^{(4)}$ IS INCLUDED FOR COMPLETENESS, BUT IN PRACTICE, ANY EVIDENCE THAT MIGHT EXIST ABOUT CAUSES THAT IMPACT NO COMPONENTS IN A FOUR-TRAIN SYSTEM WOULD BE "UNOBSERVABLE."

**Table 2.20 – Modified Impact Vectors With
Applicability Assessment and System Size Mapping
(Page 1 of 2)**

EVENT NUMBER		P0	P1	P2	P3	P4	Applicabilities	
							app_rc	app_cm
1	Actual Plant	0	1	0			0.958	
	JAF Plant	0.083	1.917	0	0	0		
2	Actual Plant	0	1	0			0.958	
	JAF Plant	0.042	0.479	0.599	0.24	0		
3	Actual Plant	0	1	0	0	0	0.958	
	JAF Plant	0.042	0.958	0	0	0		
4	Actual Plant	0	0.8	0.2	0	0	0.958	0.6
	JAF Plant	0.425	0.46	0.115	0	0		
5	Actual Plant	0.9	0.1	0	0	0	0.958	
	JAF Plant	0.042	0.096	0	0	0		
6	Actual Plant	0.7	0	0.2	0	0.1	0.958	0.6
	JAF Plant	0.425	0	0.115	0	0		
7	Actual Plant	0.9	0.1	0	0	0	0.958	
	JAF Plant	0.042	0.096	0	0	0		
8	Actual Plant	0	1	0	0	0	0.958	
	JAF Plant	0.042	0.958	0	0	0		
9	Actual Plant	0	0.8	0.1	0.1		0.958	0.6
	JAF Plant	0.425	0.429	0.178	0.058	0.017		
10	Actual Plant	0.8	0.2	0	0		0.958	
	JAF Plant	0.042	0.192	0	0	0		
11	Actual Plant	0	1	0	0	0	0.958	
	JAF Plant	0.042	0.958	0	0	0		

**Table 2.20 – Modified Impact Vectors With
Applicability Assessment and System Size Mapping
(Page 2 of 2)**

EVENT NUMBER		P0	P1	P2	P3	P4	Applicabilities	
							app_rc	app_cm
12	Actual Plant	0	1	0	0	0	0.833	
	JAF Plant	0.167	0.833	0	0	0		
13	Actual Plant	0	1	0	0	0	0.958	
	JAF Plant	0.042	0.958	0	0	0		
14	Actual Plant	0	0.7	0.1	0.1	0.1	0.833	0.6
	JAF Plant	0.5	0.35	0.05	0.05	0.05		
15	Actual Plant	0	0	1	0	0	0.833	0.6
	JAF Plant	0.5	0	0.5	0	0		
16	Actual Plant	0.9	0.1	0	0	0	0.958	
	JAF Plant	0.042	0.096	0	0	0		
17	Actual Plant	0	1	0			1	
	JAF Plant	0	0.5	0.625	0.25	0		
	JAF Average Impact Vector	2.99	9.21	2.153	0.588	0.122		

CHAPTER 3

QUANTIFYING MAINTENANCE IMPACT ON RISK: CASE STUDIES

Chapter 2 develops a model for quantifying the impact of changes in maintenance practices on common-cause failure rates. In this chapter, the impacts of a number of maintenance program changes (relative to the current JAF program) on RHR pump CCF rates, Q_k ($k = 1, 2, 3, 4$), are quantified. The current JAF maintenance program is described in Appendix B. The set of Q_k is propagated through the JAF plant risk model to evaluate the impact of maintenance changes on plant risk. The plant risk model is provided in Appendix C.

The case studies discussed in this chapter are developed by examining the maintenance program block diagram provided in Figure A.1, identifying possible values for each block's characteristic parameters, establishing base case parameter values to represent the JAF maintenance program, and postulating changes in these base case values (to represent changes in the maintenance program).

3.1 MAINTENANCE PROGRAM BLOCK OPTIONS

Four blocks in Figure A.1 are considered for changes. Some of the other blocks (e.g., Block 10 – QA/QC) can be treated using the approach used for the selected blocks. The treatment of still others (e.g., Block 4 – Measure of Overall Plant Effectiveness) requires a detailed analysis of plant organization and management, and is beyond the tools and data used in this study. The blocks considered are:

- **Block 1 – Maintenance Management**

- **Block 2 – Corrective, Preventive, and Predictive Maintenance**
- **Block 8 – Personnel Qualification and Training**
- **Block 9 – Procedures and Regulatory Constraints**

The following subsections present the various changes postulated for each block.

3.1.1 Block 1 – Maintenance Management

This block includes planning, scheduling, staffing, and shift coverage. These activities can affect the proximity (in time) of testing and maintenance activities on identical equipment and the crew composition during these activities. These factors can affect the likelihood of a common-cause failure affecting multiple RHR pumps.

The options affecting the Q_k are as follows:

- A) Staggered testing on two loops; use the same staff for both loops.
- B) Staggered testing on four trains; use the same staff for all trains.

The current practices at JAF are best represented by (A). This option, 1A, is used in the baseline case.

3.1.2 Block 2 – Corrective, Preventive, and Predictive Maintenance

This block indicates the degree to which corrective, preventive, and predictive maintenance are emphasized. Note that predictive maintenance can be viewed as a more efficient approach for scheduling preventive maintenance. Increased

preventive maintenance can reduce the likelihood of initial faults; its effect on preventing the coupling of faults is less clear but may still be positive.

The options affecting the Q_k are:

- A) Emphasis on corrective maintenance. Some application of preventive and predictive maintenance.
- B) Emphasis on preventive maintenance. Some application of predictive maintenance.
- C) Emphasis on predictive maintenance.

The current practices at JAF are best represented by (A). This option, 2A, is used in the baseline case.

3.1.3 Block 8 – Personnel Qualification and Training

The qualifications and training of personnel clearly can affect the likelihood of common-cause failures and of RHR train restoration errors.

The options affecting the Q_k are as follows:

- A) Maintenance crew is not trained in specific procedure for RHR pumps/trains.
- B) Maintenance crew is trained in specific procedure for RHR pumps/trains.

The option best representing current practices at JAF is B. This option, 8B, is used in baseline case.

3.1.4 Block 9 – Procedures and Regulatory Constraints

The availability of procedures and the quality of these procedures can affect the likelihood of common-cause failures and of RHR train restoration errors. Good quality procedures are easy to understand and easy to follow. They employ short and clear statements, and frequently employ second checks. Procedures needing improvement are long and ambiguous, and do not employ second checks.

The options affecting the Q_k are as follows:

- A) Procedures used, procedure quality needs improvement.
- B) Procedures used, procedure quality good.

The option best representing the current practices at JAF is (A). This option, 9A, is used in baseline case.

3.2 EFFECTS OF MAINTENANCE PROGRAM CHANGES ON Q_k

Using the approach developed in Chapter 2, the common cause unavailability of a group of k RHR pumps (fail to start mode), Q_k , is computed for a variety of cases. The results are shown in Table 3.1.

The first case treated in Table 3.1 is a baseline analysis, intended to represent the current practices at JAF. The JAF program is characterized in terms of the options described in the preceding section. Thus, for example, considering Block 1 (Maintenance Management) the current JAF policy is to stagger the testing of RHR loops (instead of staggering the testing of the separate trains). This is common cause failure (CCF) Option A for that block. Table 3.1 provides both brief

descriptions of the options, and a code for these options (which represents the block number and the relevant option for that block).

The next two cases represent the best and worst available combinations of CCF options. The following intermediate cases are nearly identical to the baseline case, with the exception that one option is allowed to vary. It can be seen that the α_3 and α_4 factors change relatively more than the other factors. ϕ_d , Q_3 and Q_4 can be significantly reduced by maintenance program changes; the best case leads to roughly a factor of 15 reduction in Q_3 , a factor of 25 reduction in Q_4 and a factor of 30 reduction in ϕ_d . These reductions are due to the model's assessment of the effect of an increased emphasis on predictive maintenance and improved procedures for RHR pump maintenance. The worst case results in somewhat smaller increases in ϕ_d (a factor of 3) Q_3 (a factor of 2) and Q_4 (a factor of 3). The difference between this case and the baseline case involves crew training; the baseline case assumes that the crew is trained specifically on the RHR pump maintenance procedures; the worst case assumes they are not so trained. The changes in ϕ_d , Q_3 and Q_4 predicted for the intermediate cases are generally small, varying from the baseline prediction by a factor of 2 to 3 for ϕ_d , Q_3 and Q_4 .

3.3 EFFECTS OF MAINTENANCE PROGRAM CHANGES ON PLANT RISK

Table 3.2 presents the impact on plant risk for each case. The risk model used is provided in Appendix C. Also presented in Table 3.2 is the prediction of the preliminary JAF Individual Plant Examination. The JAF result differs slightly from the baseline case result of this study due to this study's treatment of JAF-specific factors that affect common cause failure (e.g., training), and due to differences in the common cause failure model used (this study uses the α -factor model; the JAF

study uses the β -factor model).

Even though Q_4 is a significant contributor to risk, and can change significantly with different maintenance practices, Table 3.2 shows that the changes in plant risk for the different cases tend to be small. In particular, the potential for risk improvement appears to be quite small. This situation arises because of a well-known characteristic of PRAs: although Q_4 is significant contributors to risk, it is not the only contributor. As measures are taken to reduce the RHR common cause failure rate, other (previously less important) contributors become visible. On the other hand, the results for the worst case indicate that, if maintenance activities affecting the RHR pumps are significantly degraded, there can be a mild increase in risk.

The detailed results in Table 3.2 clearly depend upon the modeling assumptions employed in Chapter 3 and Appendix C, and upon the assumptions made in assessing the baseline conditions at the JAF plant.

Table 3.1 – Common Cause Failure Cases (Page 1 of 2)

Case Name	Definition	$\hat{\phi}_d$	α_k	Q_k
Baseline CCF	Staggered testing on two loops; Use the same staff for both loops; Emphasis on corrective maintenance, Some preventive and predictive maintenance; Maintenance crews trained specifically in RHR procedures; Procedure quality needs improvement. Code: (1A, 2A, 8B, 9A)	0.005	$\alpha_1 = 0.763$ $\alpha_2 = 0.178$ $\alpha_3 = 0.049$ $\alpha_4 = 0.01$	$Q_1 = 0.003$ $Q_2 = 4.7 \times 10^{-4}$ $Q_3 = 1.9 \times 10^{-4}$ $Q_4 = 1.6 \times 10^{-4}$
Best CCF	Staggered testing on four trains; Use the same staff for all trains. Emphasis on predictive maintenance. Maintenance crews trained specifically in RHR procedures. Good procedure quality. Code: (1B, 2C, 8B, 9B)	1.6×10^{-4}	$\alpha_1 = 0.794$ $\alpha_2 = 0.153$ $\alpha_3 = 0.047$ $\alpha_4 = 0.006$	$Q_1 = 2 \times 10^{-4}$ $Q_2 = 2.6 \times 10^{-5}$ $Q_3 = 1.2 \times 10^{-5}$ $Q_4 = 6.2 \times 10^{-6}$
Worst CCF	Staggered testing on two loops; Use the same staff for both loops. Emphasis on corrective maintenance; Some preventive and predictive maintenance. Maintenance crews not trained specifically in RHR procedures. Procedure quality needs improvement. Code: (1A, 2A, 8A, 9A)	0.0155	$\alpha_1 = 0.781$ $\alpha_2 = 0.168$ $\alpha_3 = 0.038$ $\alpha_4 = 0.013$	$Q_1 = 0.009$ $Q_2 = 0.001$ $Q_3 = 4.6 \times 10^{-4}$ $Q_4 = 6.1 \times 10^{-4}$

Table 3.1 - Common Cause Failure Cases (Page 2 of 2)

Case Name	Definition	$\hat{\phi}_d$	α_k	Q_k
Case 1 CCF	Staggered testing on four trains; Use the same staff for all trains. Emphasis on corrective maintenance; some preventive and predictive maintenance. Maintenance crews trained specifically in RHR procedures. Procedure quality needs improvement. Code: (1B, 2A, 8B, 9A)	0.0025	$\alpha_1 = 0.782$ $\alpha_2 = 0.162$ $\alpha_3 = 0.049$ $\alpha_4 = 0.007$	$Q_1 = 0.002$ $Q_2 = 2.1*10^{-4}$ $Q_3 = 9.5*10^{-5}$ $Q_4 = 5.4*10^{-5}$
Case 2 CCF	Staggered testing on two loops; Use the same staff for both loops. Emphasis on preventive maintenance. Maintenance crews trained specifically in RHR procedures. Procedure quality needs improvement. Code: (1A, 2B, 8B, 9A)	0.003	$\alpha_1 = 0.763$ $\alpha_2 = 0.179$ $\alpha_3 = 0.048$ $\alpha_4 = 0.01$	$Q_1 = 0.002$ $Q_2 = 2.4*10^{-4}$ $Q_3 = 9.6*10^{-5}$ $Q_4 = 8.4*10^{-5}$
Case 3 CCF	Staggered testing on two loops; Use the same staff for both loops. Emphasis on predictive maintenance. Maintenance crews trained specifically in RHR procedures. Procedure quality needs improvement. Code: (1A, 2C, 8B, 9A)	$1.8*10^{-3}$	$\alpha_1 = 0.764$ $\alpha_2 = 0.18$ $\alpha_3 = 0.046$ $\alpha_4 = 0.011$	$Q_1 = 0.001$ $Q_2 = 1.6*10^{-4}$ $Q_3 = 6.2*10^{-5}$ $Q_4 = 5.8*10^{-5}$
Case 4 CCF	Staggered testing on two loops; Use the same staff for both loops. Emphasis on corrective maintenance; some preventive and predictive maintenance. Maintenance crews trained specifically in RHR procedures. Good procedure quality. Code: (1A, 2A, 8B, 9B)	$1.8*10^{-3}$	$\alpha_1 = 0.769$ $\alpha_2 = 0.173$ $\alpha_3 = 0.05$ $\alpha_4 = 0.009$	$Q_1 = 0.001$ $Q_2 = 1.6*10^{-4}$ $Q_3 = 6.7*10^{-5}$ $Q_4 = 4.8*10^{-5}$

Table 3.2 – Cases Risk Results

Cases	Plant Risk F(TW)	Ratio to Baseline F(TW)
IPE Results	1.7*10⁻⁴	0.73
Baseline Case	2.3*10⁻⁴	1.0
Best Case	1.4*10⁻⁴	0.61
Worst Cases	4.7*10⁻⁴	2.0
Case 1	1.8*10⁻⁴	0.78
Case 2	1.9*10⁻⁴	0.83
Case 3	1.7*10⁻⁴	0.74
Case 4	1.7*10⁻⁴	0.74

Note: F(TW) is defined in Appendix C as " Frequency of loss of long term decay heat removal".

CHAPTER 4

CONCLUDING REMARKS

4.1 SUMMARY OF RESULTS

This study develops a model for quantifying the impact of maintenance program changes on common cause failure rates. This model is applied to the James A. Fitzpatrick (JAF) nuclear power plant. Seven cases are treated in the study. The baseline case represents the current JAF plant maintenance program is studied first. The other cases include best case (assuming best maintenance practices), a worst case (assuming worst maintenance practices) and intermediate cases. Significant rate reductions are found in the best case study: a factor of 30 reduction in total failure rate, a factor of 25 reduction in Q_4 (the CCF unavailability for all 4 RHR pumps) and a factor of 15 reduction in Q_3 (the CCF unavailability of a group of 3 RHR pumps). The worst case study, on the other hand, does not show a significant failure rate increases. This range of the results is believed to do with the definitions of practice levels of each maintenance activity and definitions of the baseline case activities. The former is used as fixed format of input data for the whole modeling process. The modified ccf rates are applied in the JAF plant risk model to observe the effect of different maintenance practices. The results show that the potential for significant risk reduction (or increase) due to maintenance is not extremely large; an optimal program might lead to a 60% reduction, an degraded program might lead to a factor of 2 risk increase.

4.2 ISSUES AND LIMITATIONS

As stated in Chapter 2, the approach developed in this study employs the concept of failure rate modifiers from Ref. 13. Unlike Ref. 13 (which modifies the model parameters directly), this study uses these modifiers to adjust the CCF event data base (by assessing the "applicabilities" of the events to the plant of being analyzed). The modifiers are based on industry operating experience, and need updating as more data are collected.

The analysis results clearly depend upon underlying assumptions and assessment of current plant maintenance program structure. The latter assessment involves a significant degree of analyst judgment. Before the results of this analysis are used to improve the JAF maintenance program, therefore, it is important that the assessment of the program be reviewed by persons knowledgeable about the JAF maintenance program.

4.3 APPLICATIONS

The analytical approach developed in this study can be applied to assess the impact of maintenance changes on common cause failures of any kind of components. Thus, it can be used to help design a maintenance program optimized from the standpoint of safety and cost. Consider an hypothetical example. One of the input parameters to the model is whether the plant maintenance is primarily corrective, preventive, or predictive. The model can quantify the CCF rate associated with these three different emphases, and the resulting risk. If there is no large difference between the preventive maintenance and predictive maintenance results (assuming other factors remain the same), the plant manager may decide to stay with the current preventive maintenance program, saving the resources that might be spent on predictive maintenance on other areas of plant safety.

It is important to recognize that this study does not attempt to quantify all possible modifications to a maintenance program. The model provided in this study should be used in concert with currently available models (e.g, those dealing with the actual scheduling of maintenance activities[20]) when developing an optimized program. For example, this study suggests that increased preventive maintenance should help reduce the likelihood of failures. On the other hand, increased preventive maintenance is likely to lead to increased component downtimes due to maintenance. Program optimization therefore requires a treatment of the trade-offs between these competing effects.

4.4 FUTURE WORK

The models used in this study are relatively straightforward. Improved model could improve decision making concerning program changes. There are three areas where work needs to be done to improve the model accuracy and credibility.

The first area concerns the data used in this model. As mentioned earlier, this study relies upon values for failure rate modifiers obtained from Ref. 13. Large scale efforts to collect the data for failure rate modifiers is needed.

Second, related to the first area, the fundamental basis for the failure rate modifiers needs to be examined. Issues of aging and degradation need to be taken into account. Recall that the CCF demand failure rate has two components: Q_{ccf} and λ_{ccf} . The second term represents a Poisson model for standby CCF failure; this model may need to be changed to reflect recent advances in aging research.

The third area concerns a number of maintenance program activities not treated in this model, e.g., Block 6 in Figure A.1 (communication). Improved models and data need to be developed to assist the modeling of these maintenance activities.

REFERENCES

- [1] R.E. Barlow and F. Proschan, *Statistical Theory of Reliability and Life Testing: Probability Models, To Begin With*, Silver Spring, MD, 1981.
- [2] A. Pages and M. Gondran, *System Reliability: Evaluation and Prediction in Engineering*, North Oxford Academic, London, 1986.
- [3] E. V. Lofgren, "Probabilistic Risk Assessment Course Documentation Volume 3: System Reliability and Analysis Techniques Session A - Reliability," NUREG/CR-4350/3 of 7, August 1985.
- [4] D. H. Worledge, B. B. Chu, J. Gaertner, and W. Sugnet, "Practical Reliability Engineering Applications to Nuclear Safety," NUREG/CR-0058, Proceedings of the USNRC 12th Light Water Reactor Safety Research Information Meeting, Vol. 6, pp. 309-330, 1985.
- [5] V. Dimitrijevic, "A Methodology for Incorporating Aging in System Reliability Calculations," MIT Department of Nuclear Engineering, Ph.D. Dissertation, September 1987.
- [6] W. E. Vesely, "Risk Evaluation of Aging Phenomena: The Linear Aging Reliability Model and Its Extension," NUREG/CR-4769, April 1987.
- [7] W. E. Vesely, R. E. Kurth, S. M. Scalzo, "Evaluations of Core Melt Frequency Due to Component Aging and Maintenance," NUREG/CR-5510, June 1990.
- [8] P. K. Samanta, S. M. Wong and J. Carbonaro, "Evaluation of Risk Associated with AOT & STI Requirements at the ANO-1 Nuclear Power Plant," NUREG/CR-5200, Aug. 1988.
- [9] A. I. Siegel et al., "Maintenance Personnel Performance Simulation (MAPPS) Model Summary Description," NUREG/CR-3626, May 1984.
- [10] A.D. Swain and H.E. Guttmann "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, August 1983.
- [11] K. Credit, M. Ouyang, and N. Siu, "Risk Impact of Maintenance Program Changes," MIT Department of Nuclear Engineering, MITNE-258, January 1992.
- [12] A. Mosleh, et al., "Procedure for Treating Common Cause Failures in Safety and Reliability Studies," NUREG/CR-4780, November 1987.
- [13] H. M. Paula and G. W. Parry, "A Cause-Defense Approach to the Understanding and Analysis of Common Cause Failures," NUREG/CR-5460, March 1990.

- [14] P. K. Samanta, et al., "Degradation Modeling with Application to Aging and Maintenance Effectiveness Evaluations," NUREG/CR-5612, March 1991.
- [15] K. N. Fleming, "A Reliability Model for Common Mode Failure In Redundant Safety Systems," Proceedings of the Sixth Annual Conference on Modeling and Simulation, Pittsburgh, PA, April 23-25, 1975.
- [16] A. Mosleh and N. Siu, "A Multi-Parameter Common Cause Failure Model," Transactions of the Ninth International Meeting on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, August 17-21, 1987, Vol. M, pp. 147-152.
- [17] N. Siu and A. Mosleh, "Treating Data Uncertainties in Common Cause Failure Analysis," *Nuclear Technology*, 84, No. 3, 265-281, March 1989.
- [18] K. N. Fleming and A. Mosleh, "Classification and Analysis of Reactor Operating Experience Involving Dependent Events," EPRI NP-3967, June 1985.
- [19] M. Trojovsky, "Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants: January 1, 1972 to September 30, 1980," NUREG/CR-1205, Rev. 1, September 1981.
- [20] D.H. Worledge, B.B. Chu, J. Gaertner, and W. Sugnet, "Practical Reliability Engineering Applications to Nuclear Safety," NUREG/CR-0058, Proceedings of the USNRC 12th Light Water Reactor Safety Research Information Meeting, Vol. 6, pp. 309-330, 1985

Appendix A

Descriptions of Comprehensive Maintenance Program Blocks (Adapted from Ref. 12)

Figure A.1 identifies the elements necessary for effective maintenance of plant equipment, and links between these elements. Following are the description of each block.

- **Block 1 – Maintenance Management**

Proper management is necessary to implement an effective maintenance program. Block 1 represents the maintenance management function. This includes planning, scheduling, staffing, shift coverage and resource allocation. The planning and scheduling activity includes the development of priorities and the resolution of conflicting work paths. It also includes the coordination of support groups such as engineering and operations. In planning maintenance activities, consideration should be given to radiological exposure (Block 7); proper planning results in lower radiation exposure to workers. Attention must be paid to the availability of parts and tools (including the issue of storage), as this affects planning and scheduling. Staffing and shift coverage should be sufficient to allow for training and qualification of personnel.

Also included in Block 1 is the establishment (by corporate management) of overall maintenance policies, goals, and objectives. This is necessary for efficient planning and scheduling, resource allocation, etc. Ref. 12 points out that in the Japanese nuclear industry, these policies, goals, and objectives are developed based on ten-year maintenance plans; these plans, in turn, are developed from required annual maintenance inspections. In the French nuclear industry, maintenance is given a priority comparable to operations, allowing maintenance departments to secure necessary resources.

- **Block 2 – Corrective, Predictive, and Preventive Maintenance and Surveillance**

This block indicates different strategies for maintaining equipment. Corrective maintenance is performed when component performance is deemed unacceptable or when the component fails. When corrective maintenance is performed, it is important to identify the cause of the failure, document this cause, and feed this information back to the preventive and predictive maintenance programs. Preventive maintenance involves the performance of maintenance activities on a regular schedule, independent of the status of the equipment. Predictive maintenance employs trends obtained from surveillance testing, as well as measurements of current equipment/process parameters and properties to determine when maintenance activities should be performed (i.e., when to schedule preventive maintenance). Surveillance testing is performed to obtain inservice performance data. This data is used to monitor and determine trends in component performance. Predictive and

preventive maintenance are alternate maintenance strategies that can be used to reduce the amount of corrective maintenance performed at a plant.

Japanese nuclear power plants employ a strong preventive maintenance program. Plant shut down for periodic maintenance inspection is required after 13 months. These inspections involve the disassembly and measurement of wear of individual components. The French nuclear industry, on the other hand, emphasizes predictive maintenance. Using the expected failure times for components and assessments of the importance of the components (obtained through a general risk model), priorities for preventive maintenance are established. The German nuclear industry employ a roughly 50/50 mixture of corrective and preventive maintenance activities. Periodic inspections of systems and components are performed; a procedure for conducting these inspections has been cooperatively developed by experts from the regulators, vendors, and utilities.

- **Block 3 – Post–Maintenance Testing and Return to Service**

Post–maintenance testing is important when verifying that standby safety equipment have been properly restored to service. It can also indicate the degree to which maintenance goals are being met.

Practices regarding post–maintenance testing vary across the different bodies surveyed. In the Japanese plants following a long outage, before a plant can be returned to service, a regulatory representative must witness tests for overall performance. In the French plants, post–maintenance testing is carried out by the plant operators.

- **Block 4 – Measure Overall Effectiveness**

In order to ensure that maintenance goals are being met, there should be some measure of maintenance effectiveness. A number of measures can be used to monitor maintenance effectiveness. One measure is the number of component failures experienced over time. Some other indications include ratio of corrective to preventive maintenance, work order backlog, time to restore components after discovery of failure, and the frequency of rework on components.

Block 4 provides an important part of a feedback mechanism which tells a plant if the current maintenance program is satisfactory. Information from this block should be processed by the trending function (Block 5) and communicated to a variety of groups in the plant (Block 6).

Ref. 12 states that the Japanese utilities measure their overall maintenance effectiveness using several factors: the rate of unplanned outages, plant availability, the rate of occurrence of incidents and failures regarding safety systems, exposure of personnel, and the amount of radioactive waste material generated. These are largely the same performance indicators as employed by INPO for U.S. plants.

- **Block 5 – Equipment History and Trending**

Maintenance goals, policies and objectives should be based in part on equipment history. This block indicates how equipment history and trending analyses based on this history can be used to provide feedback to the plant useful for improving maintenance management.

Ref. 12 points out that the Nuclear Power Engineering Test Center in Japan performs root cause analyses for failures down to the train level. The French have two support groups which aid in equipment history and trending data. One group analyzes significant events and failures and maintains records on equipment life. The other group, the Groupe des Laboratories, researches equipment conditions and failure mechanisms. To avoid failures from being repeated, the French constantly update their maintenance procedures and training based on operating history.

- **Block 6 – Communication**

Block 6 provides a channel for communication between all relevant parts of the organization so that deficiencies can be corrected in a timely manner. Communication with both the corporate management and other support groups also provides for organizational learning.

Regular meetings are held in Japanese utilities to review safety measures and maintenance schedules. In the French plants, the maintenance manager reports directly to the plant manager. Since plant operations are responsible for overseeing maintenance work packages, there is a direct line of communication between these two departments.

- **Block 7 – ALARA**

Improved planning and scheduling can help reduce the time spent in high radiation areas. In France, Germany, and Japan, efforts are also being made to develop robots designed to perform maintenance in these areas.

- **Block 8 – Training**

Training directly impacts the performance of maintenance personnel, and thereby provides a condition on the planning process. Training should include both classroom and on the job training.

Training practices vary somewhat across the different groups. Japan has developed national maintenance training centers where workers receive hands-on training. The French and German utilities provide extensive in-house training of personnel. In all three countries, Ref. 12 notes that the level of experience in the maintenance area appears to be higher than in the U.S. plants, due to the former's policies of lifetime employment or promotions from within. Ref. 12 also points out that most of the management personnel in the French industry have maintenance backgrounds.

- **Block 9 – Procedures**

Like training, available procedures can affect the performance of maintenance personnel. Procedures should be technically correct and up-to-date and should be presented utilizing sound human factors principles. In Japan, specific procedures are written for each plant. In the French plants, less emphasis is placed on writing detailed procedures; there is significant reliance on the experience and qualifications of the maintenance personnel.

- **Block 10 – Quality Assurance/Quality Control**

Quality control/assurance (QA/QC) activities affect the reliability of spare parts/components used in maintenance and provide a second check on maintenance performance. In Japan, QA/QC is the primary responsibility of the manufacturer. Utilities work with the manufacturers on the design of components and the quality of the associated manufacturing processes. In the French plants, QA/QC is responsible for verification of maintenance work and review of maintenance work packages. The QA function in German groups includes keeping a list of recurrent maintenance; this list specifies the work done for a particular component and the time interval between work actions. (Note the overlap with Block 5.)

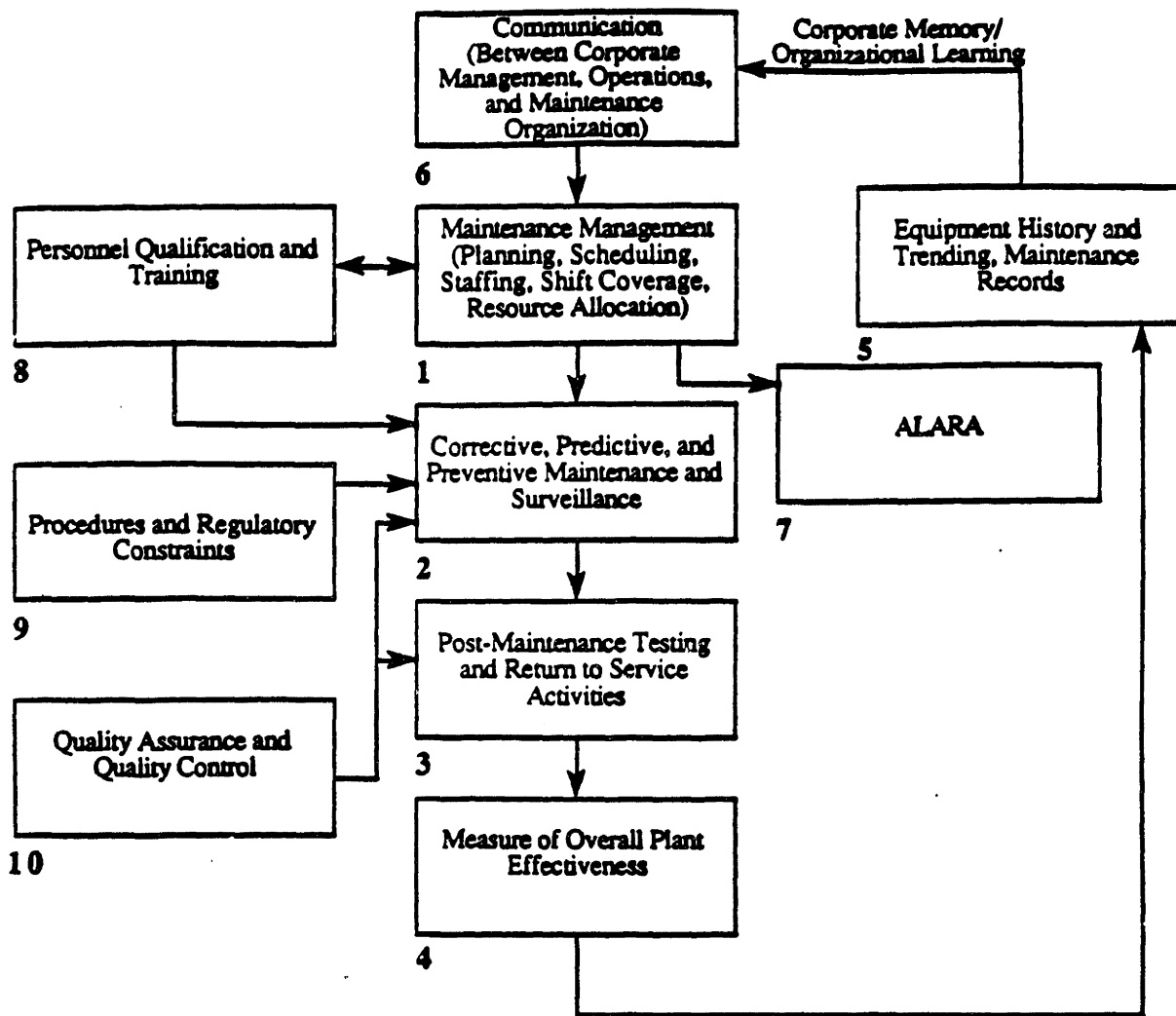


Figure A.1 Comprehensive Maintenance Program Block Diagram

Appendix B

Maintenance Program at the James A. Fitzpatrick Nuclear Power Plant

This appendix, adapted from Ref. 12, describes the current maintenance program at the JAF plant and discusses this program at the JAF plant with respect to the comprehensive program described in Figure A.1.

1 Work Request Process

The following discussion describes activities performed before and after maintenance is actually performed on a component. The activities include the planning and scheduling of maintenance activities, the coordination of support groups, post-maintenance testing, and record keeping.

The first step in the maintenance process is to generate a work request. All plant personnel can generate a work request, but most work requests are initiated by operators that identify problems in their daily rounds.

The work request is forwarded to the shift supervisor for review. The shift supervisor decides if the problem is reportable, if authorization is required, and if the work request will put the plant in a limiting condition of operation (LCO).

Next the work request is then given to quality control (QC) personnel in the work control center. The work control center is an area adjacent to the main control room. It is staffed by personnel from the operations, radiation protection services, and QC departments. The QC personnel ensure that the QA (quality assurance) category assigned by the initiator is correct and decide if a person from the QC department is needed while the work is performed.

The work request is next forwarded to the maintenance department. A clerk enters the work request into a computer system and then assigns it to a planner. Each planner is responsible for certain systems. If the job requires parts, it is designated "hold for parts" (HFP). When it is ready to be worked it is designated "ready to work" (RTW). The job is then scheduled with operations and radiation protection by the maintenance general supervisor.

A work package, including the work request, is then given to the maintenance supervisor. The package also contains work permit requests and work tracking forms. The work permit request is used to get permission to do the job. This is generally filled out by the maintenance supervisor. It provides instructional guidance for the task and pertinent historical data (from previous JAF experiences). The work tracking form gives permission to do the work. This form is filled out by a Senior Reactor Operator. It is also used by the worker to document the work performed. Sometimes, photographs of the component to be worked will be taken and included in the work package to ensure that the component can be easily identified.

Communication between the maintenance and support groups can occur in two ways. The first is provided by the activities in the work control center, as described above. The second is through daily morning meetings between

management and group supervisors. During these meetings the maintenance tasks to be carried out that day are discussed and support groups are able to provide input or concerns to the maintenance group.

Upon completion of the task, the work package is returned to the supervisor for review and then to the work control center. Operations will assess whether there is to be post-work testing. If testing is required, this is performed by operations.

When postwork testing is completed, the planners record the work history into the computer system, QC checks package for completeness, operations checks the package, and then the package is microfiched. If the work is found to be unsatisfactory during the post-work testing, another worktracking form is initiated for rework.

2 Predictive and Preventive Maintenance

The above discussion describes the process carried out for corrective maintenance. The maintenance program at JAF also includes preventive and predictive maintenance.

Most of the current preventive maintenance (PM) at JAF is based on manufacturers' recommendations. Recently, a Preventive Maintenance Tracking Force (PMTF) has been formed to review the current preventive maintenance program. The PMTF group evaluates the preventive maintenance being done on components in terms of frequency and task being performed. The group findings are intended for use in scheduling preventive maintenance to be performed on components.

The concept behind much of the work being performed by the PMTF is similar to that underlying Reliability-Centered Maintenance (discussed in the next section). In the case of the PMTF, however, the analysis is done on a component basis, e.g., all check valves, as opposed to a system basis. The intent of the PMTF is to allocate limited maintenance resources more efficiently.

Regarding predictive maintenance, a separate performance group (not in the maintenance department) provides technical services for a variety of plant components. The group provides the maintenance department with enough information to implement predictive maintenance. The group performs the following tasks:

- A. Monitoring of vibration of safety related pumps and valves.
- B. Lube oil analysis.
- C. Inservice testing – flows, differential pressures, and temperatures. These tasks are performed by daily critical equipment online monitoring, and monthly walk-around checking of safety related equipment.

If a problem is identified that is critical to plant operations, an emergency work request form is issued by the performance group. If a problem is identified

that is not critical, it is deferred to the next refueling outage.

3 Training of Maintenance Technicians

The JAF practices for staffing of maintenance technicians follows that of French and German utilities in that technicians are hired from within the company. New technicians are selected from the security guard force. A test is given and the people with the highest scores are selected to participate in the apprentice training program.

All training is done in-house. Training begins with subjects such as algebra, chemistry, and heat transfer. The training department is equipped with mock-up components so the apprentice technicians get hands-on training. At times, large components, e.g., service water pumps, may be brought in to train the technicians on. Technicians are sent to other training facilities to learn some specific skills such as welding. The training program for an apprentice also includes on the job training. As the apprentice learns and can perform certain tasks, the task is checked off a list of required skills.

After apprentice training is completed, the technician becomes a journeyman. Journeymen also receive ongoing training. If the maintenance supervisor discovers a deficiency in the performance of some task, he recommends that the training department prepare a lesson on this task. Training department personnel also keep track of incidents at other plants. The training department decides if the incident is relevant to the JAF plant. If it is relevant, a training session is given on this event.

4 Procedures

The maintenance procedures at JAF are written by a special group trained to write procedures (with an emphasis on human factors). The group is composed of experienced maintenance personnel. As in the French plants, there is some reliance on the skill of maintenance technicians in that there are not procedures for all tasks. In some cases, the technical manual for the component is judged to be sufficient for job performance.

Procedures are reviewed biannually. The procedure review is prioritized by the importance and frequency with which the procedures are used.

The results of the interviews indicate that most errors made by maintenance technicians have been due to the misinterpretation of procedures. Technicians are being trained to stop work if the procedure is unclear. Work should not be resumed until the problem is resolved. This may require going to the original procedure writer for clarification. To encourage this process, the steps for updating procedures or making temporary changes have been made easier.

5 Quality Control

The quality control department is independent of all other plant departments and groups. They report to a Quality Control group at corporate headquarters. There are three groups in the Quality Control (QC) department:

- A. Procurement – located in the warehouse; performs the purchasing of components and ensures the quality of incoming components.
- B. Auditing – assesses the quality of administrative aspects of departments such as procedures and training.
- C. Inspectors – work directly with the technicians; makes sure technicians are using proper parts and procedures.

The QC inspector watches the task being performed but does not tell the worker how to perform his job. This is to ensure that the worker will feel responsible for the quality of his work. If there is a problem with the procedure, or quality of work, QC makes recommendations to the department to make changes.

6 Comparison with Maintenance Block Diagram

A comparison of the JAF maintenance program with Figure A.1 shows that the JAF program appears to address most of the issues of interest identified in that diagram. Many of these issues are dealt with by the work request process, as described earlier. For example, this process addresses the maintenance management function (Block 1), the recording of component history (Block 5), communication between management, operations, and maintenance (Block 6), radiation protection concerns (Block 7), and QA/QC concerns (Block 10). The work request process requires interactions between the planners, who schedule equipment maintenance (and also are in charge of parts acquisition), the operations group, and the radiation protection group. The work request process also requires that when a work order is prepared, the history of the component of interest must be provided; when the work is completed, the maintenance performed on the component must be recorded in a computer system and on microfiche.

Regarding corrective, preventive, and predictive maintenance (Block 2), the work request process discussion indicates how corrective maintenance is performed. Preventive maintenance also involves the processing of a work request. Currently, the Preventive Maintenance Tracking Force is in the process of determining if components are correctly prioritized and if they are being maintained at the optimal frequency. As part of this activity, preventive maintenance requirements are also being developed. Predictive maintenance is performed by the performance group. This group performs inservice testing of components.

Post-maintenance testing (Block 3) is performed by the operations department. The decision to perform this testing is also made by the operations department.

Maintenance technicians are hired from within the company. All training is done in-house (Block 8). The technicians have both classroom and on-the-job training. The training department also monitors industry events to proactively determine if training could prevent similar occurrences at JAF (this can be viewed as fulfilling part of the function of Block 5).

Maintenance procedures (Block 9) are written by a specially trained group of

procedure writers. These writers are all experienced maintenance technicians. Procedures are updated based on their importance and frequency of use. The process for making changes in procedures has been recently updated to make it easier to change procedures. This was done to encourage technicians to suggest changes, instead of requiring them to interpret and apply poorly written or incorrect procedures.

One block in Figure A.1 apparently not addressed (at least formally) by the JAF maintenance program is Block 4. This involves the measurement (at a plant level) the effectiveness of maintenance. It is not clear from the available information if there are additional weaknesses in the depth of application of each block (e.g., in the amount of staffing for the training group) or in the interactions between the various blocks (e.g., in the communication of industry experience to other parts of the organization besides training). A comprehensive evaluation of the organizational strengths and weaknesses of the current JAF maintenance program requires more research into the detailed program structure;

Appendix C

J.A. Fitzpatrick Plant Risk Model

The risk model results in JAF Preliminary Individual Plant Evaluation document are developed using the small event tree/large fault tree approach. The model is aimed at quantifying the frequency of the "TW sequence" – the loss of long term decay heat removal. Decay heat removal capability is provided by the residual heat removal (RHR) system. At JAF, the RHR system has four RHR pumps, four RHR service water pumps and two RHR heat exchangers.

To quantify the frequency of loss of long term decay heat removal (λ_{dhr}), the document identifies 12 classes of accident initiators that can lead to loss of long term decay heat removal. These 12 classes involve either transients or LOCAs; For each of the initiators identified, dedicated event trees are constructed. These allow definition of the TW sequences in terms of the underlying systems, components, and failure modes. Following event tree quantification, the dominant sequences are identified.

Once the dominant sequences are identified, the dominant minimal cutsets (those that contribute the most to the dominant sequences) can be found. Note that although recovery factors were applied to the dominant sequences, this study focuses on the sequences prior to this application.

There are five accident initiators in those dominant sequences. They are:

- T1: Loss of Offsite Power (LOSP);
- T2: Loss of PCS Transients (MSIV, or Turbine Bypass Failure);
- TDC: Transient Caused by Loss of Safety DC Bus;
- S1: Intermediate LOCA;
- S2: Small LOCA.

In order to summarize the risk model, we define the following terms:

- F₁: total frequency of sequences with initiator of T1;
- F₂: total frequency of sequences with initiator of T2;
- F₃: total frequency of sequences with initiator of TDC;
- F₄: total frequency of sequences with initiator of S1;
- F₅: total frequency of sequences with initiator of S2;
- F(TW): total frequency of dominant TW sequences;

Using the notation λ_{ie} to represent the frequency of a specified initiating event and $\Sigma(\text{Sequence})$ to denote the sum of the probabilities of the dominant minimal cut sets for a given sequence, the simplified JAF risk model is as follows:

$$\begin{aligned} F_1 &= \lambda_{t1}[\Sigma(\text{T1-4}) + \Sigma(\text{T1-14}) + \Sigma(\text{T1-33-S3-37})] \\ F_2 &= \lambda_{t2}[\Sigma(\text{T2-4}) + \Sigma(\text{T2-34-S1-3})] \\ F_3 &= \lambda_{tdc}[\Sigma(\text{TDC A-4}) + \Sigma(\text{TDC B-4})] \\ F_4 &= \lambda_{s1} \Sigma(\text{S1-3}) \\ F_5 &= \lambda_{s2}[\Sigma(\text{S2-5}) + \Sigma(\text{S2-37}) + \Sigma(\text{S2-42})] \end{aligned} \tag{C.1}$$

and

$$F(\text{TW}) = \sum_{i=1}^5 F_i \tag{C.2}$$