NUCLEAR ENGINEERING

MASSACHUSETTS INSTITUTE
OF TECHNOLOGY

RISK IMPACT OF MAINTENANCE PROGRAM CHANGES

K. Credit, M. Ouyang, and N. Siu

MITNE–298
January 1992

RISK IMPACT OF MAINTENANCE PROGRAM CHANGES

K. Credit, M. Ouyang, and N. Siu

MITNE–298
January 1992

Nuclear Engineering Department
Massachusetts Institute of Technology
Cambridge, MA 02139

Final Report
Contract Number S–90–00196
"Operating and Maintenance Cost Reduction Using Probabilistic Risk Assessment (PRA)"

Project Officer: Herschel Specter

New York Power Authority
White Plains, NY 10601

ABSTRACT

This study quantifies the change in one measure of plant risk, the frequency of loss of long–term decay heat removal, due to changes in maintenance at the James A. Fitzpatrick (JAF) plant. Quantification is accomplished in two steps. First, the effects of maintenance are quantified in terms of changes in: a) the frequency of common cause failure of residual heat removal (RHR) pumps and b) the frequency with which operators fail to correctly restore the RHR system following maintenance. These parameters are selected as the result of an importance analysis for the plant. Second, the changes in these two parameters are propagated through a simple plant model to obtain the associated change in plant risk.

Based on this study's assessment of the current maintenance program at JAF, it appears that the potential for significant risk reduction due to improved maintenance is not extremely large; an optimal program might lead to an 80% reduction. The optimal program would place a stronger emphasis on predictive maintenance, and would employ improved procedures for RHR pump maintenance. There is potential for significant risk increase (around a factor of 70) if the maintenance program is significantly degraded (e.g., if post–maintenance is deemphasized).

This study shows how, at a simple level, maintenance program changes can be quantified without explicit modeling of the details of a plant's management and organizational structure. However, such modeling may be required: a) to more strongly justify the quantitative factors used in the analysis and b) to quantify the effect of other program changes not yet treated (e.g., the strengthening of program elements ensuring feedback of information to organization). In addition, failure data specific to the JAF plant are also needed to increase the confidence in the quantitative results of this study.

ACKNOWLEDGMENTS

The authors would like to thank N. Rasmussen and R. Su for their useful comments and discussion, and A. Hudson for her assistance with the preparation of this report. Special thanks are given to H. Specter of the New York Power Authority for his interest and patience. This report, based upon the S.M. theses of the first two authors, was prepared with the support of the New York Power Authority under contract S–90–00196, "Research for Operating and Maintenance Cost Reduction Using Probabilistic Risk Assessment (PRA)." The opinions, findings, conclusions and recommendations expressed herein are those of the authors and do not necessarily reflect the view of the New York Power Authority.

TABLE OF CONTENTS

APPENDIX A

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1 Background

It is well understood that improvements in nuclear power plant service and maintenance[1] will lead to increased plant safety. However, the quantitative degree of improvement in safety due to changes in maintenance activities, needed to determine whether these changes actually represent improvements, are not as well understood. For example, although it may be known that reducing the frequency of surveillance testing may actually reduce the wear on a given component, the associated quantitative impacts at the component, system, and plant levels of safety are not often known.

Probabilistic risk assessment (PRA) is a tool that can be used to quantify the safety impact of changes in plant maintenance. By determining the risk associated with specific changes, decision making regarding maintenance can be improved. For example, PRA can be used to help provide answers to four key questions:

- How should components be prioritized for servicing?
- Should a given component be serviced now?
- How often should a component be regularly serviced?
- To what extent should a component be serviced?

Regarding the first question, PRA can be used directly to prioritize components from the standpoint of risk. A variety of risk importance measures are available (and widely implemented) to quantify the degree to which a particular component contributes to the overall plant risk. This prioritization can also be useful if additional diagnostic instrumentation is to be installed in the plant.

PRA cannot provide a complete answer to the second question; that depends largely on the current physical condition of the component. However, PRA can be used to determine the likelihood of an accident, given the failure of the equipment. In other words, it can be used to determine if the component should be serviced immediately, or if, for example, servicing can be delayed until the next plant outage. Note that faulty decisions in this area, unsupported by PRA, have been important contributing factors to the TMI–2 accident and a number of other prominent incidents experienced by the nuclear power industry.

PRA can be used, in principle, to directly answer the third and fourth questions. An analysis can be done to determine optimal servicing intervals, and to determine the extent of servicing (e.g., to determine if the component should be repaired or replaced). Increased servicing frequency would likely lead to the decrease of certain sources of accidents, but could increase others (e.g., human errors leading to initiating events or safety system unavailability). PRA models can be used to determine the optimized tradeoff between these influences (subject to the current state of knowledge regarding the underlying processes). Ref. 1 describes a prototypical study aimed at optimizing Surveillance Testing Intervals for a standby safety system (a BWR high pressure coolant injection system) that includes the possibility of component aging, wearout due to testing, and various levels of repair/replacement effectiveness. Determination of the degree of servicing requires treatment of component aging (e.g., see [2–4]).

[1] "Service and maintenance" (henceforth called "maintenance" for brevity) covers the wide variety of activities, including support activities (e.g., scheduling), performed to ensure that plant equipment is kept at a proper level of functionality.

The qualifier "in principle" is used in the above descriptions of the potential benefits of PRA because conventional PRA applications methods are not always sufficiently advanced or detailed to quantify these benefits. This report, therefore, addresses a number of PRA methodology issues, as well as the specific application of PRA to plant maintenance.

1.2 Objective

The objective of this project is to evaluate the risk impact of potential changes in the maintenance program for the James A. Fitzpatrick plant (JAF), a Mark I BWR chosen as the case study. Achievment of this objective requires

- identification of important system failures, component failures, and component failure modes [5], and
- quantification of the impact of potential regulatory changes on the frequencies of these events.

Achievement of the first sub–objective allows the concentration of analysis resources on risk–significant issues[2]. Moreover, it also allows immediate identification of systems/components/failure modes for which changes in the associated maintenance activities will have little effect on risk. Achievement of the second sub–objective is required to determine the quantitative impact of maintenance activity changes, in order that risk–benefit comparisons can be made.

Current probabilistic risk assessment (PRA) technology is capable of satisfying the first sub–objective. Indeed, the identification of important contributors to risk is a central feature of most, if not all, current risk assessment studies. This project employs conventional importance analysis methods to identify important systems, components, and failure modes for JAF. Different presentations of the results of the importance analysis (including that suggested in Ref. 5) are investigated for their usefulness to decision makers.

On the other hand, current PRAs typically address some, but not all, issues associated with the second sub–objective. For example, methods to treat the effect of altered maintenance frequencies and durations on maintenance–induced unavailability have been previously explored (e.g., see [1]). However, changes in component failure rates due to altered maintenance programs are not quantified. The quantification portion of this project concentrates on assessing the change in the frequencies of potentially dominant risk contributors due to changes in maintenance activities; in particular, it addresses the impacts of maintenance on common cause failure rates and human error rates.

1.3 Quantitative Analysis Approach

The general approach adopted to quantify the risk impact associated with specific maintenance program changes is straightforward. Assuming that a PRA model has been constructed for the plant of interest, the plant risk is a function of the basic event likelihoods provided as input to the PRA model. Furthermore, in many PRAs, most of the basic events do not actually contribute significantly to the overall risk; only a few basic

[2] The possibility that the effects of maintenance program will be so dramatic that previously unimportant systems/components/failure modes become dominant is believed to be unlikely and is not dealt with in this report. The methods provided in the report, however, can be used to determine on a case–by–case basis if this assumption should be relaxed.

events "dominate" the risk. Thus, the analysis only needs to quantify the impact of maintenance program changes on the likelihoods of these few, dominant basic events, and to propagate these changes through the PRA model.

The four tasks implementing this approach are as follows:

- **Develop simplified system and plant models**

  As indicated above, only a relatively small number of basic events contribute significantly to the overall risk. This task involves the creation of a simplified, approximate model for the JAF plant's risk which enables rapid recalculation of plant risk after key basic event likelihoods are modified. The model is based on the dominant sequences reported in Ref. 6[3]. The task also involves the creation of a simplified model for the Residual Heat Removal (RHR) system, since the impact of maintenance program changes on the unavailability of that system are of interest.

- **Identify important components/failure modes**

  Using the simplified plant and system models, the important components are identified. This study employs the well-known Fussell–Vesely measure of basic event importance [8]. (The use of other importance measures, e.g., the "risk reduction measure," does not lead to significant differences in ranking, as discussed in Section 4.) The results of this task indicate that two basic events, the common cause failure of four RHR pumps to start on demand, and the failure of operators to restore the RHR system to its original configuration after testing/maintenance, are significant contributors to risk.

- **Quantify impact of maintenance program changes on PRA parameters**

  The results of the second task indicate that two failure modes, "common cause failure" and "failure to restore," are significant for the JAF plant. This task develops and applies simple models needed to calculate the changes in the likelihoods of these two failure modes due to postulated changes in the JAF maintenance program. Changes in common cause failure likelihood are computed using common cause failure data for RHR pumps in combination with the α–factor model [9]; changes in the probability that operators fail to restore the RHR system following maintenance are computed using the Technique for Human Error Rate Prediction (THERP) [10].

- **Propagate PRA parameter changes through models**

  This is done in a straightforward manner using the simplified plant and RHR system models developed in the first task.

[3] Ref. 6 provides risk results generated for an early risk model for JAF. Ref. 7 presents the more recently developed JAF Individual Plant Examination plant model. Due to timing considerations, this report employs the model and results of Ref. 6 as a case study; however, the general approach and some of the methods developed in this report are expected to be useful in any updated analyses of the risk impact of maintenance program changes at JAF.

1.4 Summary of Results

This report develops two simple approaches for quantifying the effect of maintenance program changes on common cause failure rates and on human error rates, respectively. These methods are applied to the James A. Fitzpatrick (JAF) plant, using a preliminary version of the JAF Individual Plant Examination to translate the changes in common cause failure and human error rates into changes in risk.

Table 1.1 summarizes the quantitative results of the analysis. A comparison of "best" and "worst" case maintenance program changes with a baseline calculation for plant risk shows that the maximum improvement that can be achieved (considering only common cause failure and human error) is roughly a 50% reduction in risk from the baseline JAF value. On the other hand, if the maintenance practices at JAF are significantly degraded, the risk can increase by up to a factor of 60.

The effect of maintenance program changes on RHR system unavailability are much smaller. This is due to the fact that, in this study, the dominant sequences are associated with loss of offsite power (LOSP) initiators; the basic events contributing the most to total RHR system unavailability are different from those contributing to RHR system unavailability when offsite power is lost.

This study shows that the impact on risk of maintenance program changes can be quantified. Although the degree of impact is not necessarily dramatic, especially when considering realistic program changes, knoweledge of the quantitative impact is nevertheless useful when optimizing a maintenance program from the standpoint of economics and safety.

1.5 Report Structure

In order to quantify the impact of potential changes in a maintenance program, the characteristics of a maintenance program must first be described. Section 2 presents the elements of a general maintenance program, and discusses how elements of this program are implemented in the French, German, and Japanese nuclear programs, and by the particular plant being used as a case study (the James A. Fitzpatrick plant. Section 2 also provides an overview of the "maintenance rule" recently issued by the U.S. Nuclear Regulatory Commission [11].

Section 3 discusses conventional methods currently used in PRA studies to assess the risk contribution associated with service and maintenance activities. It also briefly models for component failures that can be adapted to quantify partial impacts of maintenance program changes on risk, and models for human error that can be used in a similar capacity.

Section 4 provides an overview of the simplified plant and system models (based on the preliminary JAF risk study [6]) used to determine the impact on risk due to changes in basic event probabilities. This is used to quantify the risk impact of maintenance changes (which are directly manifested by changes in the basic event probabilities). Section 4 also presents a number of scoping analyses which provide order–of–magnitude estimates for the impact of maintenance.

Section 5 describes the methods used to treat the impact of maintenance program changes on common cause failure rates. The section covers the available data, the α–factor parametric model used for quantification [9], and the changes in the model parameters (the α-factors) due to specific changes in maintenance. Calculations are performed to indicate the effect of maintenance program changes on common cause failure rates and, hence, on RHR system unavailability and plant risk.

Section 6 describes the methods used to treat the impact of maintenance program changes on human error rates (the failure to restore mode). The adaptations of the THERP model used in the analysis are described. Calculations are performed to indicate the effect of maintenance program changes on human error rates and on RHR system unavailability and plant risk.

Section 7 presents the quantitative impacts on plant risk and RHR system unavailability due to a number of maintenance program changes. The effects of these changes on common cause failure rates and on human error rates, and the resulting joint effect on unavailability and risk are computed. It is shown that a number of postulated program improvements can lead to a 30% reduction in risk, and that one undesirable set of changes can lead to a fator of 90 increase in risk.

Section 8 summarizes the results of the study, discusses some of the study limitations, indicates how the results can be used in applications, and discusses where additional work is required.

Table 1.1 – Summary of Results

Case	System Unavailability Q_{rhr}	Ratio to Baseline Q_{rhr}	Plant Risk $F(TW)$[b]	Ratio to Baseline $F(TW)$
IPE Result	$5.5*10^{-3}$	0.98	$1.7*10^{-4}$	0.85
Baseline	$5.6*10^{-3}$	1.0	$2.0*10^{-4}$	1.0
Best Case	$5.4*10^{-3}$	0.96	$1*10^{-4}$	0.50
Worst Case	1	180	$1.2*10^{-2}$	60
Case 1	$5.6*10^{-3}$	1.0	$1.9*10^{-4}$	0.95
Case 2	$5.5*10^{-3}$	0.98	$1.4*10^{-4}$	0.70
Case 3	$5.5*10^{-3}$	0.98	$1.5*10^{-4}$	0.75
Case 4	$5.5*10^{-3}$	0.98	$1.3*10^{-4}$	0.65
Case 5	$5.7*10^{-3}$	0.98	$1.0*10^{-3}$	5.0

[a] See Table 7.3 for a definition of the different cases.
[b] Frequency of sequence class TW: loss of long term decay heat removal.

2. MAINTENANCE PROGRAMS AND THE MAINTENANCE RULE

In order to quantify the impact of changes in a maintenance program, it is first necessary to characterize the elements of a maintenance program. This section presents a general representation of a comprehensive nuclear power plant maintenance program. This representation is based largely on the requirements of the recently issued "Maintenance Rule;" this rule, in turn, relies to a significant extent on Ref. 12's review of maintenance practices of the French, German, and Japanese nuclear industries, as well as of the maintenance programs in the U.S. Navy and the U.S. commercial airline industry. This section also discusses the current maintenance program for the James A. Fitzpatrick (JAF) plant and provides an overview of the Maintenance Rule. Finally, two applications of PRA (or PRA–related methods) that are currently being used in the improvement of maintenance programs and that can be useful in the implementation of the maintenance rule are reviewed. The first deals with the optimization of plant technical specifications; the second, Reliability–Centered Maintenance (RCM), provides an improved method for prioritizing plant components for maintenance.

2.1 Elements of a Maintenance Program

An effective maintenance program includes more than just the actual performance of maintenance. Supporting functions are also needed to effectively perform maintenance tasks. Figure 2.1 identifies the elements necessary for effective maintenance of plant equipment, and links between these elements. This figure is based in part upon the previously mentioned review of maintenance practices in international nuclear power programs and in other industries [12].

- 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.)

2.2 Maintenance Program at the James A. Fitzpatrick Nuclear Power Plant

This section 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 Section 2.1. The program description is based on interviews with the head of the JAF maintenance department and with personnel from the JAF QA/QC department, maintenance training group, preventive maintenance tracking force, and performance group.

2.2.1 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.

2.2.2 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:

1. Monitoring of vibration of safety related pumps and valves.

2. Lube oil analysis.

3. 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.

2.2.3 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.

2.2.4 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.

2.2.5 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:

1. Procurement – located in the warehouse; performs the purchasing of components and ensures the quality of incoming components.

2. Auditing – assesses the quality of administrative aspects of departments such as procedures and training.

3. 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.

2.2.6 Comparison with Maintenance Block Diagram

A comparison of the JAF maintenance program with Figure 2.1 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.

The one block in Figure 2.1 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 (e.g., see [13]); the tools developed in this work should be useful in the quantification portion of the evaluation.

2.3 The Maintenance Rule

As stated earlier, Ref. 12 documents an NRC–conducted survey of maintenance practices in foreign nuclear plants. This study confirms the belief of the commission that good maintenance is correlated with high component reliability, low plant transient frequency, and thus, low plant risk [11]. The NRC has also performed Maintenance Team Inspections (MTIs) of U.S. nuclear power plants and concludes that although there is an improving trend in maintenance programs, there are still weaknesses that need to be addressed. Ref. 11 points out some areas of weakness, including inadequate root cause analysis leading to repetitive failures, lack of equipment performance trending, lack of consideration of plant risk in the prioritization, planning and scheduling of maintenance.

Ref. 11 states that the effectiveness of maintenance must be continuously assessed. The results of these assessments should be fed back through the plant's maintenance organization to provide requirements where inadequacies are found. In addition to the assessment of maintenance programs, the reliability of equipment should be assessed because this is also an important measure of maintenance effectiveness.

The weaknesses identified by the MTIs has led the NRC to develop a "Maintenance Rule" requiring all nuclear power plant licensees to monitor the effectiveness of maintenance. The rule will integrate risk considerations into this monitoring and provide a basis for inspection and enforcement. This rule is added to 10 CFR 50.65 and is called "Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants."

The maintenance rule requires licensees to determine maintenance goals based on safety and industry–wide operating experience. Institution of a method for assessing the degree to which these goals are being met is also required. If the goals are not being met, the rule requires that corrective action be taken.

According to the maintenance rule, the assessment of maintenance performance shall include monitoring the performance of components to ensure that they are capable of fulfilling their intended function. Ref. 11 states that monitoring can be performance oriented (e.g., reliability monitoring), condition oriented (e.g., parameter trending), or a combination of these two. The rule recognizes that not all components need to be monitored in this fashion due to their high reliability. The use of reliability–based methods, such as PRAs, for developing maintenance goals is encouraged. Monitoring may vary from system to system depending upon system importance to plant risk. Furthermore, the rule states that for the most part, monitoring can be accomplished at the system or train level. The extent of monitoring depends on the contribution of the system to the plant risk.

An annual evaluation of maintenance goals and preventive maintenance activities is required by the maintenance rule. This evaluation should take into account industry–wide operating experience. This evaluation should also assess the status of all equipment in the plant. A balance should be attained between the goals of preventive maintenance and the objective of minimizing the unavailability of equipment.

The structures, systems, and components subject to this rule include the following [11]:

1. Safety related equipment that are necessary following a design basis event to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, and the capability to prevent or mitigate the consequences of accidents.

2. Nonsafety related equipment that are relied upon to mitigate accidents or transients or are used in plant emergency operating procedures.

3. Nonsafety related equipment whose failure could prevent safety–related structures, systems, and components from fulfilling their safety–related function.

4. Nonsafety related equipment whose failure could cause a reactor scram or actuation of a safety–related system.

Ref. 11 states that it is not necessary for plants to develop a new maintenance program, only to assess their current maintenance practices and address weaknesses. Compliance with the rule is through performance or condition monitoring against appropriate goals. When these goals are not being met, corrective action shall be taken. In addition, periodic assessment of the monitoring, goals, and preventive maintenance activities shall be made to ensure that failure and unavailability of components are minimized.

The rule will take effect five years from the date of publication in the Federal Registrar. The Commission will develop a regulatory guide within two years. The utilities will then have three years for final development. The maintenance rule is not overly proceduralized and allows the utility flexibility in carrying out the rule. The final maintenance rule is a results– oriented approach to assuring that maintenance is effectively conducted at nuclear facilities.

2.4 PRA Applications to Improve Maintenance

This section discusses two separate applications of PRA or PRA–based techniques to improve a plant's maintenance program.

2.4.1 Technical Specification Improvement Using PRA

One of the earliest uses of PRA in the area of maintenance program improvement has been the assessment of the change in risk associated with changes in Allowed Outage Times (AOT) and Surveillance Testing Intervals (STI) 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 equipment) before it must be shut down; the STIs specify the frequency at which equipment surveillance tests must be performed.

Refs. 14–20 describe a number of studies for the relaxation of AOTs and/or STIs using risk–based arguments. Ref. 14 performs several case study analyses using the SOCRATES computer program [15]. The SOCRATES program uses the results of a PRA to calculate changes in risk due to changes in STIs and/or AOTs. The required inputs include the minimal cut sets describing the problem of interest, component failure rates and demand failure probabilities, technical specification requirements, and specific testing strategies for plant equipment. The code allows the treatment of dependence between tests, and includes a calculation of conditional risk (the increase in risk level when a component is known to be failed or out of service). The code also calculates the benefits from testing of redundant components during an outage. The flexible input of the SOCRATES program allows trade–off and sensitivity studies to be performed with relative ease. Often, a trade–off such as an increased AOT balanced by more frequent surveillance, can provide operational benefits without increasing the calculated risk.

In Ref. 14, different strategies are tried: 1) to establish a basis for an AOT relaxation; 2) to study special testing requirements; 3) to study trade–offs from the results of (1) and (2); and 4) to analyze modeling sensitivities. The results show that a proper combination of strategies could allow AOTs to be increased without increasing risk. The results of sensitivity studies on AOT extension show that the predicted risk level associated with an AOT extension could be 11.5% less than the base case value due to variation in the probability values for human error or test–caused failures, and up to 23% less because of possible variations in the component failure rates.

Refs. 16–20 describe a number of utility applications for relaxation of AOTs and/or STIs using risk–based arguments. Ref. 16 describes a situation where a one–time relaxation of an AOT for a steam–driven auxiliary feedwater pump was accepted on the basis that the additional risk incurred was negligible. Ref. 17 presents the NRC's acceptance of an application requesting a reduction in diesel generator surveillance testing and an extension of the diesel generator AOTs; the acceptance was based on a demonstration that the risk associated with the extended AOT was still lower than that for a baseline period (not involving a limiting condition of operation). Ref. 18 presents a proposal to extend AOTs and STIs for 22 Technical Specifications. The proposed changes are shown to lead to a 69% increase in the computed frequency of core damage, but it is argued that this increase is small in comparison with the uncertainties in this frequency (a factor of 10). It is interesting to note that Ref. 18 states that the assessment conservatively does not account for potential improvements in maintenance due to increased AOTs which would allow increased maintenance time for components. Less time would also be spent disassembling, assembling, testing, and returning equipment to service, and there would be reduced opportunity for human error. (It is hoped that these issues will be addressed in this research project.) Ref. 19 presents the NRC's acceptance of an application requesting extended AOTs for a swing diesel generator; the acceptance is based on a computation showing that the increase in risk associated with the extended AOT is negligible. Finally, Ref. 20 presents an NRC analysis supporting acceptance of applications for increased AOTs for a number of safety systems, and rejection of applications for increased AOTs for a number of other safety systems. The acceptance and rejection arguments are both based on the degree of risk change associated with the extended AOTs.

Ref. 1 presents a methodology for assessing the impact of modified AOTs and STIs, and applies this methodology to a particular plant. In the case of AOTs, it is recognized that AOTs are direct sources of unavailability. Thus, since Ref. 1 does not account for potential reductions in component failure rates (postulated in Ref. 18 due to increased time for maintenance), increased AOTs lead to increased unavailability. Ref. 1 calculates the increase in system unavailability using simple models, propagates this increase through the overall risk model to determine the increase in core damage frequency. For the plant of interest, it is determined that the increase in core damage frequency is significant in some cases, and insignificant in others.

Increased STIs will lead to reduced detection of standby failures, reduced downtime due to testing, reduced test–related degradation, and reduced likelihood of test–related failures. The first effect will tend to increase the overall risk; the last three will tend to reduce the risk. Ref. 1 treats only the first effect. As in the case of AOTs, when the methodology is applied to the plant of interest, the computed increase in risk due to increased STIs is determined to be significant in some cases, and insignificant in others.

Refs. 1 and 14–20 show that acceptable arguments for relaxing plant Technical Specifications can be made on the basis of negligible risk impact, even though potential risk reduction benefits are not treated. Quantitative approaches for assessing these benefits are likely to prove useful in further optimization of the Technical Specifications.

2.4.2 Reliability–Centered Maintenance

One interesting non–regulatory application of PRA technology towards the improvement of a plant's maintenance program is reliability–centered maintenance (RCM). RCM, developed in the naval and aircraft industries in the late 1960's, is being investigated by EPRI for its potential use in the nuclear industry. Studies for Florida Power and Light's Turkey Point Units 3 and 4, Duke Power's McGuire Station, and Southern California Edison's San Onofre Units 2 and 3 have been used to demonstrate the benefits of RCM (including economic gains).

RCM systematically identifies those maintenance–related tasks which prevent failures from occurring and are cost–effective in regard to "safety and economic consequences" [21]. The first step in the RCM process is to define the system boundaries. The analyst should work with plant personnel to define the system. The definition of the system should include the subsystems of the system being analyzed.

Before any analyses are begun, the operating histories of the system and its components are studied. Past surveillance tests, maintenance records, and interviews with maintenance personnel aid in this process. The present preventive maintenance program is also studied to determine if preventive maintenance accounts for the reliability of components.

The significant functions of the system and the functional failures are then identified. This is done using a Functional Failure Analysis (FFA). The FFA gives the description, the interfaces, and the functional failures of the system.

The next step in the RCM process is to determine a suitable methodology to analyze each functional failure. In some cases the functional failure may not need to be analyzed further, because it may be determined to be a non–critical failure. The methods use to analyze a functional failure are quantitative or qualitative. The quantitative approach makes use of a fault tree model or a GO model. With both of these tools, the importance of component failures can be calculated allowing the ranking of components. A Failure Modes and Effects Analysis (FMEA) gives a qualitative analysis of functional failures. The dominant failure modes and their effects are identified for each functional failure. A Logic Tree Analysis is performed for each dominant failure mode considered to have a significant effect. The Logic Tree Analysis ranks the failures as high, medium, or low criticality depending on the answers to several questions involving the effect of the failure.

With the quantitative approach, the dominant failures are identified. However to develop an effective preventive maintenance program, the failure modes of those failures considered to be critical to system reliability must be explicitly determined. In the studies performed, those failures with an importance greater than 0.1 were considered to be of high criticality. A failure modes analysis must be performed for all critical failures to determine the failure modes.

In order to develop a preventive maintenance program, interviews are conducted with maintenance personnel regarding the dominant failure modes found in the RCM analysis. There are three types of preventive maintenance tasks: time directed, condition directed, and failure finding. The time directed task is one in which a schedule is set up for performing maintenance. (In an analogous situation, the oil in a car will be changed every 3000 miles.) The condition directed task involves maintenance based on specific standards. (Continuing the analogy, the oil might be changed based on its color or viscosity.) Failure–finding tasks are basically surveillances that find hidden failures and correct them. Based on input from maintenance personnel, it is decided which type of task will best prevent each dominant failure from occuring.

2.5 Summary and Comments

A comprehensive maintenance program involves a variety of supporting activities, as well as the actual performance of maintenance. Figure 2.1 illustrates the different program elements of a maintenance program, and the interactions between these elements. A comparison of the current James A. Fitzpatrick maintenance program with Figure 2.1 shows that most of the elements in the latter are covered at least to some extent. However, Block 4, which represents the evaluation of the effectiveness of the maintenance program at a plant level, is not implemented. It appears that this block will need to be addressed in response to the recently issued "Maintenance Rule" [11].

In order to develop a maintenance program optimized from the standpoint of plant safety, it is important to assess the risk impact associated with the different implementations of the basic maintenance program elements. A number of these program elements can be directly treated in a conventional PRA model. For example, as discussed in Section 3, changes in the scheduling of maintenance activities (included in Block 1, "Maintenance Management") will lead to changes in computed component/system unavailabilities whenever standby failures are treated explicitly. Reductions in average repair times, due perhaps to improved availability of parts (included in Block 1) or to improved personnel training (included in Block 8, "Personnel Qualification and Training"), and reductions in human error rates due to improved procedures for returning equipment to service (included in the Block 3, "Post–Maintenance Testing") can also be directly treated, if data are available.

Other program elements are more difficult to treat in a conventional PRA. For example, it is difficult to specify the degree to which maintenance–related human error rates should change as a result of a modified training program, or how common cause failure rates should be modified to reflect an increased emphasis on preventive maintenance. These issues, and related topics, are addressed in later sections of this report.

This page intentionally left blank.

This page intentionally left blank.

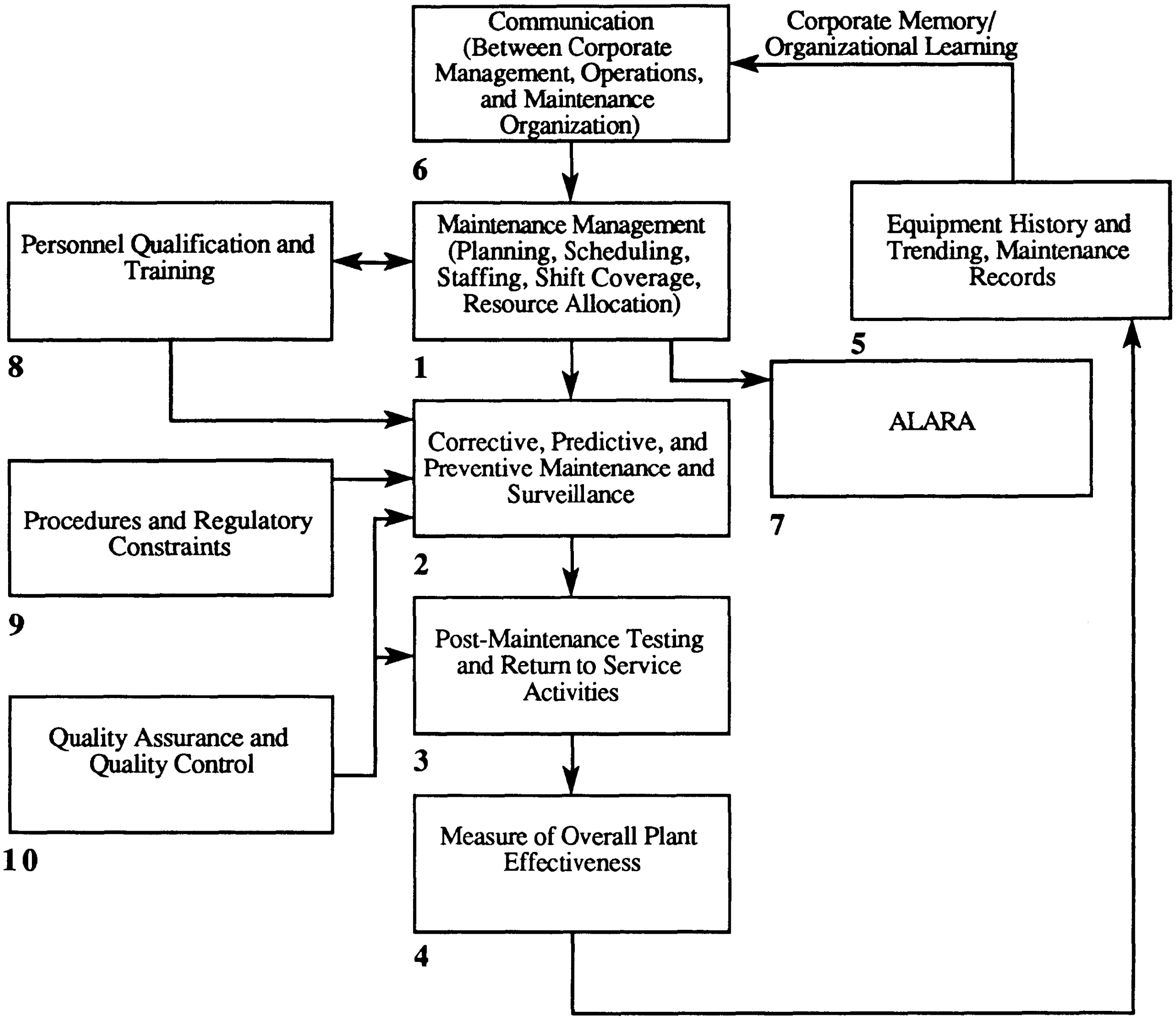

Communication (Between Corporate Management, Operations, and Maintenance Organization)
6
Corporate Memory/ Organizational Learning
Personnel Qualification and Training
8
Maintenance Management (Planning, Scheduling, Staffing, Shift Coverage, Resource Allocation)
1
Equipment History and Trending, Maintenance Records
5
ALARA
7
Corrective, Predictive, and Preventive Maintenance and Surveillance
2
Procedures and Regulatory Constraints
9
Post-Maintenance Testing and Return to Service Activities
3
Quality Assurance and Quality Control
10
Measure of Overall Plant Effectiveness
4

Figure 2.1 - Comprehensive Maintenance Program Block Diagram

3. 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.

3.1 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 given by [22][4]

$$Q_r = \frac{\tau_r}{\tau_f + \tau_r} \qquad (3.1)$$

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 [23]), 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 3.1. 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:

[4] Assuming that the component is restored to "as–good–as–new" conditions after maintenance.

$$Q_s(t) = \begin{cases} Q_d + \lambda_s t & 0 \leq t \leq T - \tau_{tm} \\ 1 & T - \tau_{tm} \leq t \leq T \end{cases} \tag{3.2}$$

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):

$$Q \equiv \frac{1}{T}\int_0^T Q(t)dt \tag{3.3}$$

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

$$Q_s \doteq Q_d + \frac{\lambda_s T}{2} + \frac{\tau_{tm}}{T} \tag{3.4}$$

(assuming that $T >> \tau_{tm}$). Note that it is common practice in PRA to separate the contributions of hardware failures and human errors to the demand unavailability Q_d [24], 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,

$$Q_s \doteq \phi_h + \frac{\lambda_s T}{2} + f_t\tau_t + f_m\tau_m + Q_{he} \tag{3.5}$$

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. This last term is a function of the frequency with which testing/maintenance is performed, the conditional frequency that an error is committed given that testing/maintenance is performed (ϕ_{he}), and the length of time required to detect the error (τ_d):

$$Q_{he} = f_t\phi_{he,t}\tau_{d,t} + f_m\phi_{he,m}\tau_{d,m} \tag{3.6}$$

If an error arising during testing is not detected until the next test and an error arising during maintenance is not detected until the next maintenance, then $f_t\tau_{d,t} = 1$ and $f_m\tau_{d,m} = 1$. In this case,

$$Q_{he} = \phi_{he,t} + \phi_{he,m} \tag{3.7}$$

It should be pointed out that Eqs. (3.5)–(3.7) apply 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. 15. 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. (3.2) and (3.5), 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).

3.2 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/maintenence.

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 3.2). The time–dependent unavailability of the system is given by

$$Q_{sys}(t) = \begin{cases} (Q_d + \lambda_s t)^2 + (Q_{ccf} + \lambda_{ccf} t) & 0 \lesssim t \lesssim T - 2\tau_{tm} \\ (Q_d + \lambda_s t) & T - 2\tau_{tm} \lesssim t \lesssim T \end{cases} \tag{3.8}$$

where, as in Eq. (3.2), the Q_d term includes hardware failures and human error, and the subscript "ccf" denotes common cause failure[5]. The term τ_{tm} is the duration of the testing/maintenance period for one component. Note that the second line in Eq. (3.8) treats the conditional unavailability of one component, given that the other component is unavailable due to testing/maintenance.

Using Eqs. (3.3) and (3.8), the average unavailability for this system is approximated by (assuming that $\tau_{tm} << T$):

$$Q_{sys} \doteq \left\{[Q_d^2 + Q_d(\lambda_s T) + \frac{(\lambda_s T)^2}{3}] + (Q_{ccf} + \frac{\lambda_{ccf} T}{2})\right\} + (Q_d + \frac{\lambda_s T}{2})(\frac{2\tau_{tm}}{T}) \tag{3.9}$$

[5] Human errors, or course, are a source of common cause failures. In this report, "common cause failure analysis" refers to the analysis of dependent failures that are not modeled explicitly elsewhere in the PRA.

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

$$Q'_{sys} \doteq \left\{ [Q_d^2 + Q_d(\lambda_s T) + \frac{(\lambda_s T)^2}{4}] + 2(Q_d + \frac{\lambda_s T}{2})(\frac{\tau_{tm}}{T}) + (\frac{\tau_{tm}}{T})^2 \right. \tag{3.10}$$

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. (3.9)]. Comparing Eqs. (3.9) and (3.10), 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.

Refs. 25 and 26 provide several expressions for M/N systems under simultaneous, sequential, and staggered testing policies. Ref. 27 develops a model for the unavailability of a periodically tested component with general failure, testing, and repair time distributions. Optimal test intervals, based on exponentially distributed failure times (also assumed in this section) are derived. Note that these results do not include demand or common cause failures.

3.3 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. (3.) and (3.10). Some changes can be modeled very simply. Increases in the frequency of testing, for example, can be treated by increasing f_t in Eq. (3.) and reducing T (since increased testing leads to a reduced detection time and a reduced likelihood of standby failures). Other changes, however, require more analysis. Changes in the failure parameters ϕ_h, λ_s, Q_{ccf}, λ_{ccf}, and ϕ_{he} are of particular interest.

The following two sections discuss current work on the modeling of λ_s and ϕ_{he}. The first 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. The common cause failure terms, Q_{ccf} and λ_{ccf}, are the subject of this study (the impact of maintenance on these parameters has not yet been treated in other studies).

3.3.1 Modeling the Standby Failure Rate λ_s

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 accomodate aging effects, the failure rate must be allowed to vary as a function of time.

In Ref. 4, the linear aging model described in Ref. 28 is implemented in a time-dependent fault tree program (FRANTIC-LA) to compute the effects of component aging on system availability. The failure rate is expressed as follows:

$$\lambda(t) = \lambda_0 + at \tag{3.11}$$

where λ_0 is the initial failure rate and the parmeter "a" is the aging acceleration parameter. In the absence of repair, it can be easily shown that the corresponding time–dependent unavailability is given by

$$Q(t) = 1 - \exp\left\{-(\lambda_0 t + \frac{1}{2}at^2)\right\} \tag{3.11}$$

Ref. 4 applies this model to periodically tested components. It allows different treatment of renewal options. The model also allows the user to change component aging parameters during plant life. In turn, this allows the modeling of different aging scales for every component, as a function of the time when the component was first introduced into service, 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. 4 allows detailed modeling of the test and repair processes; not only does it treat the time required for performing tests and repairs, it also incorporates the probability of test–caused failures, the probability that test–overrides do not function on demand, and test–interval dependent failure rates (i.e., the discontinuous changes in failure rate with the number of tests performed).

Ref. 4 applies the linear aging model to the analysis of an Auxiliary Feedwater System (AFWS) of a PWR, and a High Pressure Coolant Injection System (HPCIS) and Low Pressure Coolant Injection System (LPCIS) of a BWR. The results show that over a 60 year time period, the resulting system unavailability can be a factor of 4 to 8 greater than that predicted by a conventional PRA[6].

Ref. 4 also studies the impact of testing and maintenance on the aging–related unavailability of piping systems. Not surprisingly, it is shown that good–as–new testing and repair has the maximum effectiveness with regard to detecting and correcting aging contributions. Two other renewal strategies also shown to be capable of controlling aging effects are: 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. For example, after 60 years, piping unavailability without testing is 30 times larger than the unavailability when testing is performed once a year.

Ref. 2 studies core melt frequency changes due to aging. Let the component unavailabilities, structure failure probabilities, and initiating event frequencies be represented by the generic parameter Q. Changes in Q, denoted by δQ, are related to the aging rate and plant maintenance policy using a linear aging model. When a component is periodically overhauled, replaced, or otherwise renewed, at intervals of L with no intermittent checking for aging effects, then Eq. (3.11) indicates

$$\delta Q(L) \doteq \frac{1}{2}aL^2 \tag{3.12}$$

When surveillances are performed in–between overhauls to determine the extent of aging, Ref. 2 shows that the comparable result is

$$\delta Q = \frac{1}{4}a(L - T) + \frac{1}{6}aT^2 \tag{3.13}$$

[6] This result depends naturally on the values used for the aging parameters.

where T is the surveillance interval. Ref. 2 also shows how the change in core melt frequency can be simply computed, using the δQ's calculated from Eq. (3.13) and sensitivity coefficients derived from simple importance calculations. Using these results, maintenance activities can be prioritized based on their contribution to core damage.

Note that in Eqs. (3.12) and (3.13), the component is assumed to be restored to as good as new conditions after a time period L. After a time period T (after a surveillance), the component is assumed to be operational. 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. 29 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. 29 can provide a more robust analyses of maintenance effectiveness. Such analyses can be used when responding to the Maintenance Rule, discussed in Section 2.

Ref. 29 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. The unavailability results are used as input for PRA models to determine system and plant effects. The plant average core melt frequency is shown to be reduced by a factor of 2.6 to 4.1, while the peak core melt frequency can be reduced by a factor of 9.0 to 11.3.

3.3.2 Modeling the Human Error Rate ϕ_{he}

A number of models have been developed for human reliability analysis. This section discusses the Technique for Human Error Rate Prediction (THERP) [10], which is representative of models currently used in PRAs and is used in this study, a simplified methodology developed for use in recent PRAs [30], and the Maintenance Personnel Performance Simulation (MAPPS) [31]. MAPPS provides an example of improved human reliability analysis models that may be used in future PRAs.

3.3.2.1 THERP Methodology [10]

The THERP methodology employs 5 steps. First, the analyst must define the task of interest, what constitutes failure, and what human actions can lead to this failure. This involves the identification of the different subtasks that must be performed by the operators. A tree diagram is constructed to represent possible sequences of successes and failures in performing the different subtasks. Figure 3.3 provides an example THERP tree. In this figure, the lowercase letters represent successful performance of the subtask; the uppercase letters represent failure.

Second, the basic error rates relevant to the tree are determined. In general, the error rates are obtained from Ref. 10. The estimated error rates provided in Ref. 10 are based on experience from the nuclear power and defense industries. In Figure 3.3, for example, estimates are obtained for p{a}, the probability with which the maintainers use procedures, p{B | a}, the probability of an error given that procedures are used, and p{B | A}, the probability of an error given that procedures are not used[7]. Not surprisingly, the Ref. 10 estimate for p{B | a}, 0.003, is lower than the estimate for p{B | A}, 0.005.

The basic human error rates given in the tables provided in Ref. 10 are for tasks performed under average industry conditions. In the third step, other factors, called Performance Shaping Factors (PSFs), are introduced to account for stress, work environment, etc.

Fourth, once the basic error rates, as modified by the appropriate PSFs, are established, the analyst needs to determine if there are dependencies between the subtasks that would tend to increase the probability of multiple failures. For example, consider a task in which several level transmitters are to be calibrated. If the same technician is responsible for calibrating all transmitters, the probability that an error is made for two transmitters is greater than the square of the basic error probability for miscalibration.

Ref. 10 defines five levels of dependence: zero dependence (ZD) low dependence (LD), medium dependence (MD), high dependence (HD), and complete dependence (CD). Let F_n denote an error at the nth step/subtask in a task, and F_{n-1} denote an error at the (n–1)st step/subtask. These five levels of dependence are operationalized as follows:

$$\begin{aligned} P\{F_n | F_{n-1}, ZD\} &= \phi \\ P\{F_n | F_{n-1}, LD\} &= \frac{1 + 19\phi}{20} \\ P\{F_n | F_{n-1}, MD\} &= \frac{1 + 6\phi}{7} \\ P\{F_n | F_{n-1}, HD\} &= \frac{1 + \phi}{2} \\ P\{F_n | F_{n-1}, CD\} &= 1 \end{aligned} \qquad (3.14)$$

where ϕ is the modified error rate (including the effect of the PSFs).

In the final step, the sequence probabilities for the failure sequences in the THERP tree are summed to obtain the probability of failure for the task.

3.3.2.2 ASEP Methodology [30]

The human reliability analysis methodology described in Ref. 30, called the Accident Sequence Evaluation Program (ASEP) methodology, is a simplified version of the THERP methodology. This method is designed to be used by systems analysts who do not have training in human reliability analysis.

The ASEP methodology employs a relatively small number of rules for probability assignments. A basic human error rate of 0.03 is assumed for all latent human errors (errors that are undetected until the associated component or system is demanded). Most recovery factors (which model the probability that the operators will discover and remedy an error in time) are assigned a value of 0.9. The probability that a crew will fail to perform a post–maintenance test correctly is assigned a value of 0.01.

[7] The "human error probabilities" referred to in Ref. 10 correspond to the conditional frequencies used in this report. The terminology "frequency" is used to indicate situations where the uncertainties are stochastic rather than state–of–knowledge.

The treatment of dependence between tasks performed by the same person is different in the ASEP methodology as compared with the THERP methodology. If actions are performed on components in a series system, the actions are considered to be independent (i.e., zero dependence is assumed between the actions). Figure 3.4 is used to determine the level of dependence between actions performed on components in a parallel system. As can be seen in Figure 3.4, errors of commission and errors of omission are treated differently. Errors of commission are assumed to have a zero level of dependence. Errors of omission are assumed to have either zero, high, or complete dependence.

Several recovery factors can be used in the analysis of latent human errors. However, credit is not allowed for all recovery factors in all cases. Ref. 30 presents tables showing which recovery factors can be applied in each case. Recovery factors are applied to the following situations:

- errors are indicated by a compelling signal (e.g., an annunciator)
- post–maintenance testing is performed that will identify an error
- a written checkoff list is provided to verify component status after task completion
- there is a requirement for a check every shift or every day of component status inside or outside of the control room using a written checklist.

Once the appropriate recovery case and level of dependence between subtasks are determined, a look–up table in Ref. 30 is used to determine the joint human error probability for the task.

3.3.2.3 The MAPPS Model [31]

Ref. 31 describes the Maintenance Personnel Performance Simulation (MAPPS), a computer simulation program designed to provide maintenance oriented human performance data for PRA purposes.

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. MAPPS allows for the simulation of up to five job specialties: instrumentation and control technician, maintenance mechanic, electrician, supervisor, and quality control technician.

Figure 3.5 shows the basic algorithm used by MAPPS to determine the probability of success on a task. The analyst inputs the basic ability levels of the technicians performing the task and the parameters characterizing the task. These latter include:

- quality of written procedures for supporting performance,
- accessibility of equipment to worked on, and
- the need to wear protective clothing.

These parameters are used to determine the level of ability (intellectual and perceptual) required to perform a given task. Algorithms are used to modify the technicians' basic ability levels as a function of their current states and the working conditions; the following factors are among those treated:

- technician fatigue,
- high environment temperature,
- fatigue relief due to rest breaks,

- technician's level of aspiration,
- time since the team members last performed the task,
- organizational climate, and
- whether the actual manning is greater/less than that nominally required.

The sum of the team members' ability levels is compared with the ability requirements for the task. The difference between total ability available and ability required is then used as one of four components in computing the task success probability.

The other three components in the calculation involve stress. They are: time stress, communication stress, and radiation stress. Time stress arises when the time required to perform all remaining tasks is greater than the time available for total task completion. (Note that the process is nonlinear, since the time required to perform a task can change with stress.) Radiation stress arises when the absorbed radiation dose for a technician is greater than 800 millirem. Communication stress increases in direct proportion with noise level in the work area, the length of communications, and the number of technicians in the group. The total stress on a technician is calculated as the sum of the component stresses; the total stress on a maintenance crew is computed as the sum of the stresses on the individual technicians.

Subtracting the total team stress (minus an input threshold level) from the total team ability (minus the ability requirements of the task), the ability difference for a task, ΔD, is obtained. The probability of failure is obtained using a data–based correlation:

$$\phi = \frac{e^{\Delta D + 2.95}}{1 + e^{\Delta D + 2.95}} \tag{3.15}$$

In order to account for the inherent variability in the impact of the identified factors on an individual's ability and stress, MAPPS establishes upper and lower stochastic bounds and utilizes Monte Carlo sampling to choose a particular effect for a given individual. The distribution for team performance characteristics (e.g., task duration) are obtained by repeated sampling.

3.4 Summary and Comments

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., [2,29]) shows considerable promise in addressing this issue. However, common cause failures, which are dominant contributors to risk, have not yet been addressed, and models for human errors during maintenance, which can also be significant contributors to risk, have not yet been applied to quantify the impact of maintenance program changes on risk[8].

This project employs simple models for common cause failures and human errors during maintenance to address these problems. These models are discussed in Sections 4 and 5 of this report.

[8] Human errors, or course, are a source of common cause failures. In this report, "common cause failure analysis" refers to the analysis of dependent failures that are not modeled explicitly elsewhere in the PRA.

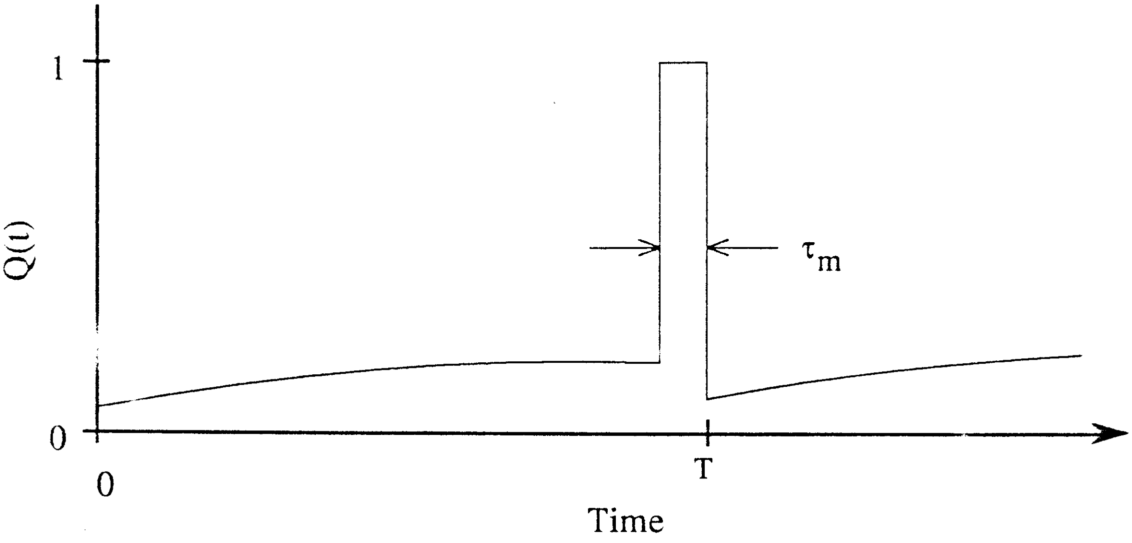


Figure 3.1 - Time-Dependent Component Unavailability

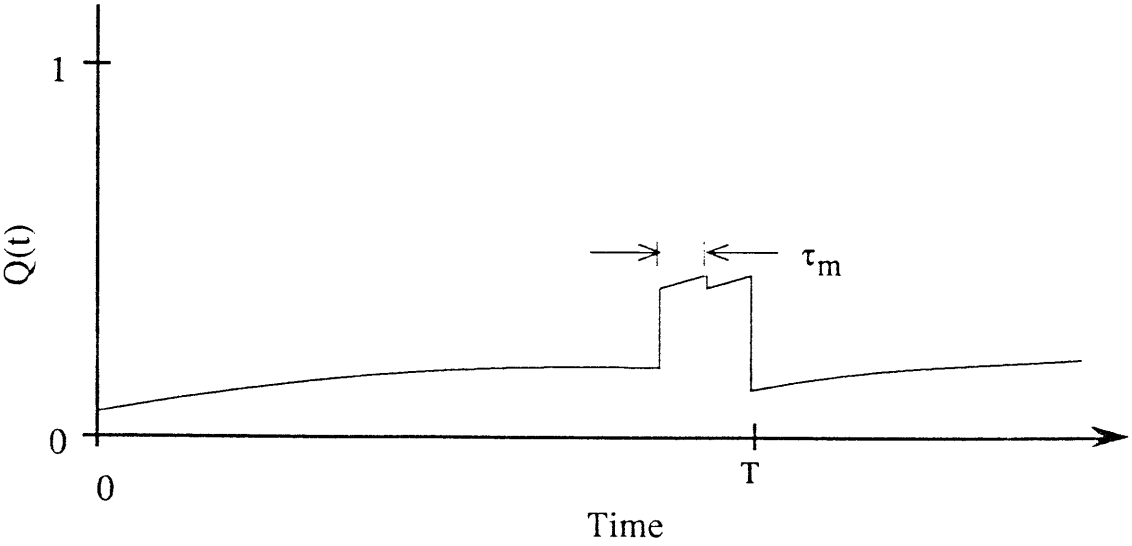


Figure 3.2 - Time-Dependent System Unavailability
(2 Pumps, Staggered Testing)

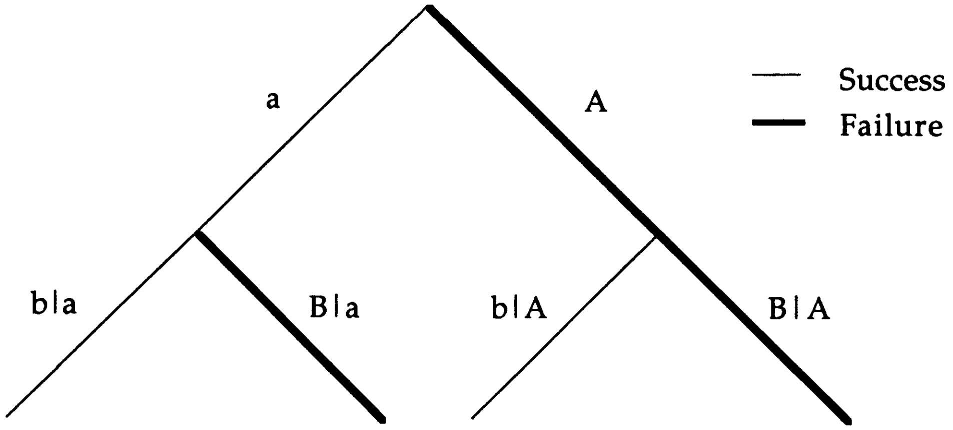


Figure 3.3 - Simple THERP Tree

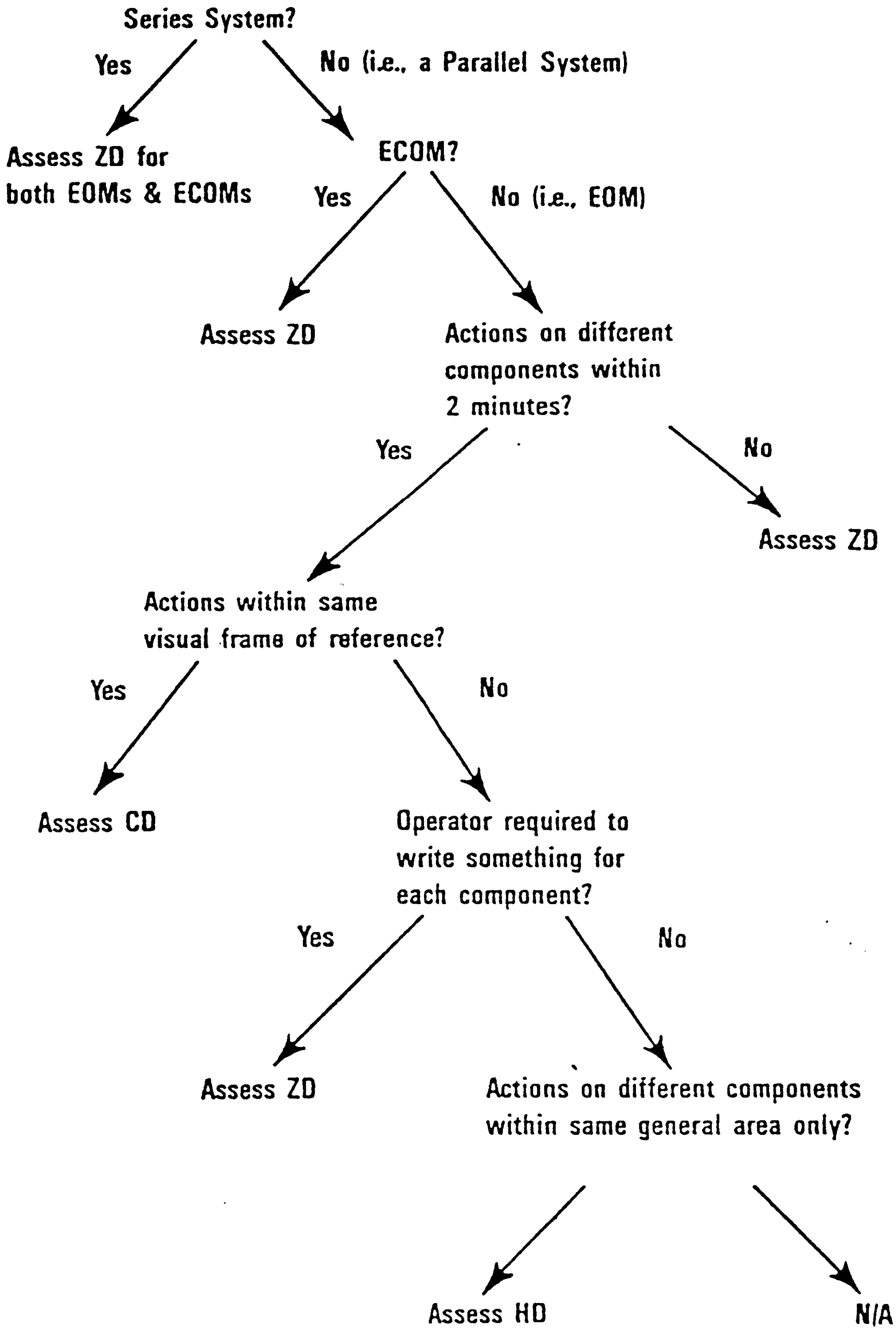


Figure 3.4 - ASEP Dependency Analysis

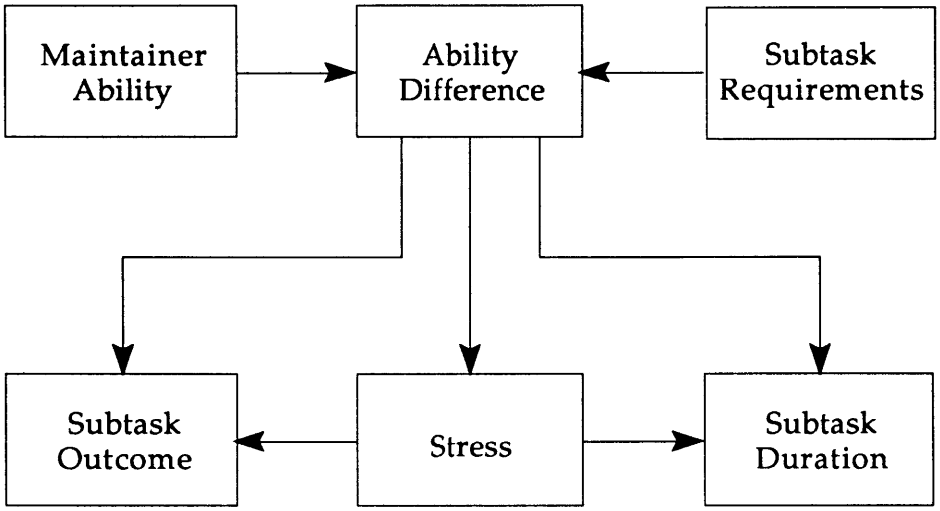


Figure 3.5 - MAPPS Analysis Methodology [31]

4. SIMPLIFIED JAF PLANT MODEL AND SCOPING CALCULATIONS

In general, a change in plant risk associated with changes in maintenance can be computed in two steps. First, the parameters for the plant PRA model (e.g., the maintenance frequency f_m) are modified to reflect the change in maintenance. Next, the plant model is requantified, using the modified parameter values as input. The problem with this procedure, if carried out too mechanically, is that requantification of the entire plant model can require significant computational resources. Moreover, since many of the parameters may have little impact on overall risk, complete requantification is not really required.

This section presents a simplified plant model suitable for use in sensitivity studies. The model is based on the dominant sequences (and the minimal cutsets for these sequences) presented in Ref. 6, a preliminary risk study for the James A. Fitzpatrick (JAF) plant[8]. An importance analysis is applied to the simplified plant model, in order to determine the dominant basic events contributing to plant risk. Two particular basic events, the common cause failure of 4 RHR pumps, and the failure of operators to properly restore an RHR train following maintenance, are found to be significant. Using these basic events, a number of scoping calculations are performed to determine the potential magnitude of changes in risk due to changes in maintenance.

4.1 Simplified Plant Model

4.1.1 Plant Risk Model

The risk model results in Ref. 6 are developed using the small event tree/large fault tree approach. (Ref. 32 provides the modeling assumptions underlying the results of Ref. 6.) The model is aimed at quantifying the frequency of the "TW sequence" – the loss of long term decay heat removal. (The purpose of Ref. 6 is to provide supporting information on the desirability of installing a filtered/venting system for the containment.) 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}), Ref. 6 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; Table 4.1 shows the initiators and their frequencies. For each of the initiators identified in Table 4.1, 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. Table 4.2 shows the 11 dominant sequences identified and their frequencies. (The cut–off frequency used in the quantification process is $1.0*10^{-9}$/yr.)

Once the dominant sequences are identified, the dominant minimal cutsets (those that contribute the most to the dominant sequences) can be found. For example, Table 4.3 shows the dominant minimal cutsets associated with the T2–4 sequence (prior to recovery).

[8] Ref. 7 presents the more recently developed JAF Individual Plant Examination plant model. Due to timing considerations, this report employs the model and results of Ref. 6 as a case study; however, the general approach and some of the methods developed in this report are expected to be useful in any updated analyses of the risk impact of maintenance program changes at JAF.

Note that although recovery factors were applied to the dominant sequences in Ref. 6, this study focuses on the sequences prior to this application.

It can be seen that there are five accident initiators in these 11 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:

- F_1: total frequency of sequences with initiator of T1;
- F_2: total frequency of sequences with initiator of T2;
- F_3: total frequency of sequences with initiator of TDC;
- F_4: total frequency of sequences with initiator of S1;
- F_5: 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 Σ(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:

$$\begin{aligned} F_1 &= \lambda_{t1}[\Sigma(T1{-}4) + \Sigma(T1{-}14) + \Sigma(T1{-}33{-}S3{-}37)] \\ F_2 &= \lambda_{t2}[\Sigma(T2{-}4) + \Sigma(T2{-}34{-}S1{-}3)] \\ F_3 &= \lambda_{tdc}[\Sigma(TDCA{-}4) + \Sigma(TDCB{-}4)] \\ F_4 &= \lambda_{s1}*\Sigma(S1{-}3) \\ F_5 &= \lambda_{s2}[\Sigma(S2{-}5) + \Sigma(S2{-}37) + \Sigma(S2{-}42)] \end{aligned} \qquad (4.1)$$

and

$$F(TW) = \sum_{i=1}^{5} F_i \qquad (4.2)$$

4.1.2 Comparison with Current Plant Model

As mentioned earlier, the plant model used in this study is based on a preliminary version of the Individual Plant Examination (IPE) study documented in Ref. 6. The primary differences between the preliminary study and the final study documented in Ref. 7 are as follows:

- Ref. 6 is an analysis focused on the endstate "Loss of Long Term Decay Heat Removal." The final IPE is a focused on core damage.
- The frequencies of the accident initiators are reduced in Ref. 7.
- The frequencies of the dominant accident sequences are reduced in Ref. 7.
- The risk–dominant common cause failure events and human errors are different in the two studies.

The fourth bullet is an expected consequence of the first; the second and third bullets are also expected, since most PRA studies involve a continual, iterative refinement of their parameter values and submodels.

It is not expected that the difference in results between the two studies require any modifications of the general methodology employed in this study to quantify the impact of maintenance on common cause failures and on human error rates. However, this study's emphasis on common cause failures and on failures to restore equipment after maintenance does depend on the results of Ref. 6; therefore, the detailed methods developed might require modification to deal with the updated model.

4.2 Ranking of Systems, Components, and Failure Modes

In order to properly focus maintenance resources on those systems, components, and component failure modes most critical to safety, some indication of the "importance" of these entities is required. This section discusses a number of the more prominent importance measures that have been suggested in the literature (some of which are routinely calculated by current PRA computer codes)[9]. Additional discussions on importance analysis can be found in Refs. 22 and 33–35.

4.2.1 Importance Measures

The basic question of how important a particular component (or component failure mode) is to risk can be asked in a number of different ways. For example, if the maximum possible reduction in risk associated with replacing a component by a perfectly good component is desired, the "risk reduction worth" is the appropriate importance measure to use. If the maximum possible increase in risk associated with replacing a component by a perfectly bad component is desired, the "risk achievement worth" is the appropriate importance measure to use. If the relative contribution of a component's unavailability to overall risk is desired, either the Fussell–Vesely importance measure or the "criticality importance measure" are appropriate.

This section presents five measures: the risk reduction worth, the risk achievement worth, the Birnbaum structural importance, the criticality importance, and the Fussell–Vesely importance. The following notation is employed (largely based on that used by Ref. 34):

$g[Q(t)]$	Baseline "risk" at time t
$Q_i(t)$	Unavailability of component i at time t
$Q_{mcs\text{-}j}(t)$	Unavailability of minimal cut set j at time t
$g[0_i,Q(t)]$	Conditional "risk" at time t, given that component i is available (i.e., that $Q_i = 0$)
$g[1_i,Q(t)]$	Conditional "risk" at time t, given that component i is unavailable (i.e., that $Q_i = 1$)

Note that the risk function, $g[\cdot]$, can represent the likelihood of loss of decay heat removal, core damage, or of system failure, as well as the likelihood of adverse public health consequences.

[9] The variety of measures stems from the fact that the fuzzy notion of "importance" can be stated mathematically in a number of different ways. It is important to note that none of the measures is clearly superior to the rest for all possible system configurations. Furthermore, as pointed out by Ref. 32, the different measures can lead to significantly different rankings of components and systems. As a result, current importance analyses tend to use a number of different measures, rather than a single one.

4.2.1.1 Risk Reduction Worth

This importance measure reflects the change in risk when component i is replaced by a "perfectly good" component. Using an interval scale,

$$I_i^{RI}(t) \equiv g[Q(t)] - g[0_i,Q(t)] \tag{4.3}$$

Using a ratio scale,

$$I_i^{RR}(t) \equiv \frac{g[Q(t)]}{g[0_i, Q(t)]} \tag{4.4}$$

4.2.1.2 Risk Achievement Worth

This importance measure reflects the change in risk when component i is replaced by a "perfectly bad" component. Using an interval scale,

$$I_i^{AI}(t) \equiv g[1_i,Q(t)] - g[Q(t)] \tag{4.5}$$

Using a ratio scale,

$$I_i^{AR}(t) \equiv \frac{g[1_i, Q(t)]}{g[Q(t)]} \tag{4.6}$$

4.2.1.3 Birnbaum Structural Importance

This measure can be viewed as a combination of the interval–based risk reduction worth and risk achievement worth measures.

$$I_i^{B}(t) \equiv g[1_i,Q(t)] - g[0_i,Q(t)] \tag{4.7}$$

It is interesting to note that when the components in the system are independent, this measure can be computed as the derivative of the risk function with respect to Q_i:

$$I_i^{B}(t) = \frac{\partial g[Q(t)]}{\partial Q_i(t)} \tag{4.8}$$

The risk reduction worth, risk achievement worth, and Birnbaum structural importance measures are easy to compute and appear to have nice intuitive meanings. It should be cautioned, however, that their use may lead to seemingly non–intuitive results. For example, the Birnbaum measure, when applied to a parallel system, will indicate that the component with the highest unavailability is the least important. Ref. 22 shows that this result is due to the fact that the Birnbaum measure gives the probability that the system is in such a state that component i is "critical", i.e., that it is in a state such that the failure of component i can change the system state. A small value of Q_i implies that the system is very likely in a state where component i is critical. This result underlines the fact that different ways of asking whether or not a component is importnat can lead to different answers.

4.2.1.4 Criticality Importance

This measure is related to the Birnbaum structural importance measure. However, this measure looks at the relative importance of a component:

$$I_i^{CR}(t) \equiv \{g[1_i,Q(t)] - g[0_i,Q(t)]\} * \frac{Q_i(t)}{g[Q(t)]} \tag{4.9}$$

which, in the case of independent components, becomes

$$I_i^{CR}(t) = \frac{Q_i(t)}{g[Q(t)]} * \frac{\partial g[Q(t)]}{\partial Q_i(t)} \tag{4.10}$$

These equations show that the criticality importance is a fractional sensitivity measure, indicating the relative likelihood that the system is in a state where component i is critical to system failure at time t.

4.2.1.5 Fussell–Vesely Importance

This measure indicates that a component is important if it appears in a large number of minimal cut sets (MCS).

$$\begin{aligned} I_i^{FV}(t) &\equiv \frac{P\{\text{at least one MCS containing i is failed}}{g[Q(t)]} \\ &\approx \frac{\sum_j Q_{mcs\text{-}j}}{g[Q(t)]} \end{aligned} \tag{4.11}$$

Here, a component can be important to risk without being "critical." Unlike the Birnbaum structural importance measure, this measure states that all components in a parallel system are equally important.

4.2.2 Application to JAF Preliminary IPE

With the information provided by the minimal cutsets for the dominant sequences, the ranking of systems, components, and failure modes with respect to their contributions to plant risk can be accomplished. In this study, the Fusell–Vesselly importance measure is used for the ranking calculations, due to its simplicity of application to this problem.

Table 4.3 provides the contributions to plant risk (loss of long term decay heat removal) associated with each basic event in the simplified plant model. The basic events are organized by system. The contribution for basic event i, P_i, is calculated as follows:

$$P_i = \sum_j \lambda_j \sum_k P\{MCS_k | i \epsilon k\} \tag{4.12}$$

where λ_j is the frequency of initiating event j and $P\{MCS_k | i \epsilon k\}$ is the probability of the kth minimal cutset of which basic event i is a member.

Using the data in Table 4.3, the Fussell–Vesely measure for system, component, and failure mode importance can be easily computed. These results are provided in Tables 4.4 through 4.19. An importance matrix, summarizing these results, is shown in Table 4.20.

The format of the table is largely as suggested in Ref. 5. Efforts to calculate changes in risk due to changes in maintenance can concentrate on the important components/failure modes shown in this table. (The contributions from components/failure modes not appearing in the table are not necessarily ignored; they can, however, probably be adequately treated using sensitivity analyses rather than specific models.) Table 4.21 shows the total frequency of the important TW sequences.

The following results can be observed from the importance matrix:

- Common cause failures are the most important contributors to plant risk. This can be seen from the fact that in the global ranking, common cause failure events hold the top two positions in the matrix.

- Human Error is the second most important contributor to plant risk. The particular error, Failure to Restore, is the third most important failure mode in the global ranking.

- Among the component groups, the pump component group is the most significant contributor to plant risk. The valve component group is the next most important.

- The RHR system (LPCI mode) is the most important system.

Based on these results, the bounding calculations described in the following section, and the detailed calculations aimed at quantifying the risk impact associated with changes in maintenance, focus on: 1) the common cause failures of RHR pumps, and 2) the failure of operators to restore the RHR system after maintenance. The latter failure, or course, is a form of common cause failure. The term "common cause failure analysis" is used to refer to the statistical analysis of dependent failures that are not modeled explicitly elsewhere in the PRA. (Restoration errors following maintenance, failures caused by external events, and failures caused by the failure of support systems are examples of dependent failures that are modeled explicitly in most PRAs studies.)

4.3 Scoping Calculations

The purpose of the scoping calculations discussed in this section is to quickly determine how much an assumed stricter (relaxed) maintenance practice aimed at a specific component/failure mode can reduce (increase) the plant risk. According to Eqs. (4.1) and (4.2), the effect can be assessed by appropriately modifying the probabilities of the minimal cutsets in the dominant sequences.

It should be pointed out that many changes in maintenance practices could have a global effect on plant components. This will not only affect several minimal cutset probabilities, it could also affect the initiating event frequencies. This study does not investigate the impact of maintenance program changes on initiating event frequencies. However, it is interesting to observe that, in the case of Loss of Main Feedwater initiators, Ref. 36 indicates that their frequency might be reduced by a factor of 2 if service and maintenance are improved.

The scoping calculations are performed as follows:

1) Identify the minimal cutsets which have the failure events of the interest (e.g., common cause failures of RHR pumps);

2) Set the probabilities of these cutsets to zero to account for the maximum possible improvement due to improved (stricter) maintenance;

3) Multiply the probabilities of these cutsets by a variety of values (> 1) to parametrically account for relaxed maintenance (note that setting the probability of a cutset to one would lead to the occurrence of the sequence with a frequency equal to the frequency of the initiating event);

4) Calculate the plant risk from (2) and (3) and compare these values with the baseline value. In this case, the frequency of loss of long term decay heat removal is

$$F(TW) = 1.7*10^{-4}/\text{reactor year}$$

4.3.1 Risk Reduction

Five calculations are performed to bound the potential impacts of various improvements in maintenance.

- Assume that perfect maintenance practices could eliminate all common cause failure events completely. In this case, the probability of all minimal cutsets including common cause failure (CCF) events can be set to zero. There results:

  $$F(TW\ \text{without CCF}) = 9.5*10^{-5}/\text{reactor year}$$

  The risk reduction factor (dividing this value by the baseline risk value) is 1.77.

- Assume that perfect maintenance practices could eliminate all human errors completely. In this case, the probability of all minimal cutsets including human error can be set to zero. There results:

  $$F(TW\ \text{without human error}) = 1.3*10^{-4}/\text{reactor year}$$

  The risk reduction factor is 1.3.

- Assume that perfect maintenance practices could eliminate all pump component related failure events completely. In this case, the probability of all minimal cutsets including pump failure events can be set to zero. There results:

  $$F(TW\ \text{without pump failures}) = 8.8*10^{-5}/\text{reactor year}$$

  The risk reduction factor is 1.9.

- Assume that perfect maintenance practices could eliminate all valve component related failure events completely. In this case, the probability of all minimal cutsets including valve failure events can be set to zero. There results:

  $$F(TW\ \text{without valve failures}) = 1.2*10^{-4}/\text{reactor year}$$

  The risk reduction factor is 1.5.

- Assume that perfect maintenance practices could eliminate all RHR system hardware related failure events completely. In this case, the probability of all minimal cutsets including any RHR system hardware failure events can be set to zero. There results:

F(TW without RHR system hardware failure) = $1.0*10^{-4}$/reactor year

The risk reduction factor is 1.6.

It can be seen that the maximum decrease in risk, even for the most important systems, components, and failure modes is around a factor of 2.

4.3.2 Risk Increase

A number of calculations are performed to gauge the potential impacts of various relaxations in maintenance that end up increasing the frequency of common cause failure and human error. Some samples for the results are provided below.

- Assume that the RHR pump CCF rate is increased by a factor of 5. There results:

  F(TW: CCF increased by a factor of 5) = $2.8*10^{-4}$/reactor year

  The risk increase factor is 1.7.

- Assume that the RHR pump CCF rate is increased by a factor of 10. There results:

  F(TW: CCF increased by a factor of 10) = $4.3*10^{-4}$/reactor year

  The risk increase factor is 2.5.

- Assume that the RHR pump CCF rate is increased by a factor of 100. There results:

  F(TW: CCF increased by a factor of 100) = $3.0*10^{-3}$/reactor year

  The risk increase factor is 18.

- Assume that the failure to restore rate is increased by a factor of 5. There results:

  F(TW: HE increased by a factor of 5) = $3.4*10^{-4}$/reactor year

  The risk increase factor is 2.0.

- Assume that the failure to restore rate is increased by a factor of 10. There results:

  F(TW: HE increased by a factor of 10) = $5.6*10^{-4}$/reactor year

  The risk increase factor is 3.3.

- Assume that the failure to restore rate is increased by a factor of 100. There results:

  F(TW: HE increased by a factor of 100) = $4.0*10^{-3}$/reactor year

  The risk increase factor is 24.

The effect on risk due to increases/decreases in the probabilities of common cause failure and human error are shown in Figures 4.1 and 4.2. Not surprisingly, the plant risk increases nearly linearly with both the RHR pump CCF rate and the human error rate. This relationship is due to the importance of these parameters in the risk model.

4.3.3 Areas for Improvement

From the above scoping calculations, it can be seen that the most effective method for risk reduction is one that reduces the probabilities of pump component failure events. The next choice is a method that reduces the probability of common cause failure events. Figure 4.2 shows the results of additional scoping calculations where the common cause failure rates are reduced by factors of up to 1000. It can be seen that with a increase in reduction factor from 2 to 10, there is a (relatively) rapid risk reduction. When the reduction factor is near 1000, the resulting risk is nearly equal to the risk calculated when the common cause failures are completely eliminated.

The scoping calculations identify areas where improved maintenance can have the largest impact. The next problem is to see what maintenance improvements can actually lead to the hypothesized reductions in common cause failure and human error rates. This is discussed in the following two sections.

4.4 Summary and Comments

Using the dominant sequences and minimal cutsets identified in the preliminary IPE for JAF, a simple risk model is constructed. (Because this study uses Ref. 6 as a basis, the consequence of interest in this project is loss of long term decay heat removal, rather than core damage.) This risk model is then used to determine the order of magnitude of possible changes in plant risk due to changes in maintenance that affect common cause failure rates and human error rates.

The results of the scoping calculations show that, even with fairly drastic assumptions (e.g., all pumps are rendered perfect, all common cause failure rates increase by an order of magnitude), the associated changes in plant risk are not large (from a factor of 2 risk reduction to a factor of 5 risk increase). Note that these scoping calculations are performed for important components/failure modes. Changes in the failure parameters characterizing less important components/failure modes will have significantly less impact on plant risk. Thus, if reductions or increases in risk of this order will have no effect on decision making, no additional analysis is needed to quantify the impact of maintenance changes. The models and accompanying discussion provided in the remainder of this report are relevant when these risk reductions/increases are indeed significant.

4.5 TABLES

Table 4.1 - JAF Initiating Event Frequencies

Initiator	Mean Frequency (yr^{-1})	Source
T1: Loss of Offsite Power (LOSP)	0.057	(1)
T2: Loss of PCS Transients(MSIV, or Turbine Bypass Failure)	0.48	(2)
T3A: Transients With Condenser Initially Available	4.72	(2)
T3B: Loss of Feedwater With Main Condenser Available	0.39	(2)
T3C: IORV (Inadvertently Open Relief Valve)	0.094	(2)
TAC: Transient Caused by Loss of Safety AC Bus	5.0E-3	(3)
TDC: Transient Caused by Loss of Safety DC Bus	5.0E-3	(3)
A: Large LOCA	1.0E-4	(3)
S1: Intermediate LOCA	3.0E-4	(3)
S2: Small LOCA	3.0E-4	(3)

Notes:

(1) JAF plant-specific data with Bayesian update.
(2) JAF plant-specific data from actual operating history.
(3) NUREG/CR-4550, Vol. 4, Rev. 1, Part 1, Table 4.3-3

Table 4.2 - Dominant Sequences from JAF Preliminary Model Before Recovery

Sequence	Frequency
T1-4	3.43 x 10^{-5}
T1-14	2.11 x 10^{-6}
T1-33-S3-37	9.58 x 10^{-7}
T2-4	7.58 x 10^{-5}
T2-34-S1-3	1.22 x 10^{-7}
S1-3	6.75 x 10^{-8}
S2-5	1.09 x 10^{-8}
S2-37	1.15 x 10^{-8}
S2-42	< 1.0 x 10^{-9}
TDCA-4	2.3 x 10^{-5}
TDCB-4	4.1 x 10^{-5}

Table 4.3 – Samples of T2–4 Sequence Minimal Cutsets (Page 1 of 3)

	EVENT NAME	DESCRIPTION	PROB. (Note 1)
1)	T2-4		
1)	RSW-CCF-VF-2MOVS	CCF OF RHRHX SW DISCH VLVS FAIL TO OPEN	7.01E-05
	T2	LOSS OF POWER CONVERSION SYS INITIATOR	
	U1X-SUCC	SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS	
	/C	REACTOR PROTECTION SYSTEM	
	/P	SRV'S RESEAT	
2)	LCI-CCF-PF-4MDPM	RHR PUMP COMMON CAUSE FAILURE	5.24E-05
	T2	LOSS OF POWER CONVERSION SYS INITIATOR	
	U1X-SUCC	SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS	
	/C	REACTOR PROTECTION SYSTEM	
	/P	SRV'S RESEAT	
3)	RSW-CCF-PF-4MDPS	COMMON CAUSE FAILURE OF RHRSW PUMPS	1.40E-05
	T2	LOSS OF POWER CONVERSION SYS INITIATOR	
	U1X-SUCC	SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS	
	/C	REACTOR PROTECTION SYSTEM	
	/P	SRV'S RESEAT	
4)	LCI-HTX-VF-HE-2A	LOOP A HEAT EXCHANGER E-2A FAILURE	2.85E-06
	LCI-HTX-VF-HE-2B	LOOP B HEAT EXCHANGER E-2B FAILURE	
	T2	LOSS OF POWER CONVERSION SYS INITIATOR	
	U1X-SUCC	SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS	
	/C	REACTOR PROTECTION SYSTEM	
	/P	SRV'S RESEAT	
5)	LCI-HTX-VF-HE-2B	LOOP B HEAT EXCHANGER E-2B FAILURE	1.24E-06
	T2	LOSS OF POWER CONVERSION SYS INITIATOR	
	U1X-SUCC	SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS	
	RSW-RCK-NO-MV89A	VALVE CONTROL CIRCUIT NO OUTPUT	
	/C	REACTOR PROTECTION SYSTEM	
	/P	SRV'S RESEAT	
6)	LCI-HTX-VF-HE-2A	LOOP A HEAT EXCHANGER E-2A FAILURE	1.24E-06
	T2	LOSS OF POWER CONVERSION SYS INITIATOR	
	U1X-SUCC	SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS	
	RSW-RCK-NO-MV89B	VALVE CONTROL CIRCUIT NO OUTPUT	
	/C	REACTOR PROTECTION SYSTEM	
	/P	SRV'S RESEAT	

Table 4.3 – Samples of T2–4 Sequence Minimal Cutsets (Page 2 of 3)

EVENT NAME	DESCRIPTION	PROB. (Note 1)
7) LCI-XHE-RE-PM3AP AC4-RLY-NO-HOEB3 T2 U1X-SUCC /C /P	FAIL TO RESTO PM-3A PATH CMPTS AFT MAIN LO REL 86-1HOEB03 PATH FAILURE LOSS OF POWER CONVERSION SYS INITIATOR SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS REACTOR PROTECTION SYSTEM SRV'S RESEAT	1.10E-06
8) LCI-XHE-RE-PM3AP AC4-RLY-NO-HOEB1 T2 U1X-SUCC /C /P	FAIL TO RESTO PM-3A PATH CMPTS AFT MAIN REL 86A-1HOEB01 PATH FAILURE LOSS OF POWER CONVERSION SYS INITIATOR SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS REACTOR PROTECTION SYSTEM SRV'S RESEAT	1.10E-06
9) T2 U1X-SUCC RSW-RCK-NO-MV89A RSW-RCK-NO-MV89B /C /P	LOSS OF POWER CONVERSION SYS INITIATOR SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS VALVE CONTROL CIRCUIT NO OUTPUT VALVE CONTROL CIRCUIT NO OUTPUT REACTOR PROTECTION SYSTEM SRV'S RESEAT	5.42E-07
10) LCI-HTX-VF-HE-2A AC4-RLY-NO-HOEB3 T2 U1X-SUCC /C /P	LOOP A HEAT EXCHANGER E-2A FAILURE LO REL 86-1HOEB03 PATH FAILURE LOSS OF POWER CONVERSION SYS INITIATOR SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS REACTOR PROTECTION SYSTEM SRV'S RESEAT	5.30E-07
11) LCI-HTX-VF-HE-2A AC4-RLY-NO-HOEB1 T2 U1X-SUCC /C /P	LOOP A HEAT EXCHANGER E-2A FAILURE REL 86A-1HOEB01 PATH FAILURE LOSS OF POWER CONVERSION SYS INITIATOR SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS REACTOR PROTECTION SYSTEM SRV'S RESEAT	5.30E-07

Table 4.3 – Samples of T2–4 Sequence Minimal Cutsets (Page 3 of 3)

	EVENT NAME	DESCRIPTION	PROB. (Note 1)
12)	LCI-XHE-RE-PM3DP	FAIL TO RESTO PM-3D PATH CMPTS AFT MAIN	2.69E-07
	T2	LOSS OF POWER CONVERSION SYS INITIATOR	
	U1X-SUCC	SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS	
	DC1-BDC-ST-10500	PANEL FAULTS BY ANY LOAD 10500	
	/C	REACTOR PROTECTION SYSTEM	
	/P	SRV'S RESEAT	
13)	LCI-XHE-RE-PM3DP	FAIL TO RESTO PM-3D PATH CMPTS AFT MAIN	2.69E-07
	T2	LOSS OF POWER CONVERSION SYS INITIATOR	
	U1X-SUCC	SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS	
	DC1-BDC-ST-DC-A4	PANEL FAULTS BY ANY LOAD 71DC-A4	
	/C	REACTOR PROTECTION SYSTEM	
	/P	SRV'S RESEAT	
14)	LCI-XHE-RE-PM3DP	FAIL TO RESTO PM-3D PATH CMPTS AFT MAIN	2.69E-07
	T2	LOSS OF POWER CONVERSION SYS INITIATOR	
	U1X-SUCC	SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS	
	DC1-BDC-ST-BCB2A	PANEL FAULTS BY ANY LOAD BCB-2A	
	/C	REACTOR PROTECTION SYSTEM	
	/P	SRV'S RESEAT	
15)	LCI-XHE-RE-PM3AP	FAIL TO RESTO PM-3A PATH CMPTS AFT MAIN	2.69E-07
	T2	LOSS OF POWER CONVERSION SYS INITIATOR	
	U1X-SUCC	SUCCESSFUL ALIGNMENT OF HPCI SUCT TO CS	
	DC1-BDC-ST-10600	PANEL FAULTS BY ANY LOAD 10600	
	/C	REACTOR PROTECTION SYSTEM	
	/P	SRV'S RESEAT	

Table 4.4 - Samples of T2-4 Sequence Minimal Cutsets (Page 1 of 4)

RHR Service Water (RSW)

(RSW-1): 2 MOV RHRHX SW Discharge Valves, fail to open, P_{2MOVs}= 3.8E-5

(RSW-2): RHR Pumps, fail to run, P_{4MDPS} = 7.6E-6

(RSW-3): MOV 89A Control Circuit , no output, P_{NOA} = 4.4E-6

(RSW-4): MOV 89B Control Circuit , no output, P_{NOB} = 4.4E-6

(RSW-5): Manual Switch 10A-S48B Path, fault, P_{FTB} = 5.5E-7

(RSW-6): Manual Switch 10A-S48A Path, fault, P_{FTA} = 5.5E-7

(RSW-7): Motor Driven Valve MV89B, fail to open on demand, P_{CCB}= 7.4E-7

(RSW-8): Motor Driven Valve MV89A, fail to open on demand, P_{CCA} = 7.4E-7

(RSW-9): Manual Valve 24B , fails closed (plugged), P_{PGV} = 1.6E-7

(RSW-10): Manual Valve 11B in Loop B, fails closed (plugged), P_{PG11v}= 1.6E-7

(RSW-11): Pump P-1A, fail to continue running, P_{FR1A}= 1.6E-7

(RSW-12): Pump P-1C, unavailable due to maintenance, P_{MA1C}= 1.6E-7

Table 4.4 - Plant Risk Contributions from Basic Events (Page 2 of 4)

Low Pressure Coolant Injection (LCI)

(LCI-1): PM-3A Path, fail to restore after maintenance, P_{RE3A} = 2.2E-5

(LCI-2): Loop A Heat Exchanger E-2A, fails, P_{HEAF} = 1.2E-5

(LCI-3): PM-3D Path, fail to restore after maintenance, P_{RE3D} = 2.1E-5

(LCI-4): Loop B Heat Exchanger E-2B, fails, P_{HEBF} = 1.2E-5

(LCI-5): 4 RHR Pumps, fails, P_{4MF} = 2.8E-5

(LCI-6): Motor Driven Valve MOV16A, fails to open on demand, P_{M16A}= 1.3E-8

(LCI-7): Motor Driven Valve MOV16B, fails to open on demand, P_{M16B}= 1.3E-8

(LCI-8): Relay 10A-K84A Path, fails, P_{K84A} = 4.5E-9

(LCI-9): Relay 10A-K48B Path, fails, P_{K48B} = 4.2E-9

(LCI-10): SWGR Control Circuit, no output, P_{RP-3D} = 2.3E-7

(LCI-11): Pump P-3D, stop running, P_{P-3DF} = 2.6E-10

(LCI-12): Check Valve VCM-30AN-42D, fails to open, P_{FOV} = 1.1E-6

(LCI-13): Relay 10-A-K22B, fails to remain open, P_{FRO} = 5.9E-7

(LCI-14): Manual Switch 10-S3D Path, Fails, P_{SWPF} = 1.2E-10

(LCI-15): Check Valve VCW-30AN-42B, fails to remain closed, P_{FRC}= 2.9E-6

(LCI-16): Valve MOV12B in Heat Exchanger outlet, plugged, P_{12PG} = 2.0E-7

(LCI-17): Valve MOV65B in Heat Exchanger outlet, plugged, P_{65BPG}= 2.0E-7

(LCI-18): Valve VCM-30AN-45D, fails to close, plugged, P_{45PG}= 1.6E-7

(LCI-19): Check Valve VCM-30AN-42C, fails to stay close, P_{FSC} = 2.9E-6

(LCI-20): SWGR Control Circuit RP-3A, no output, P_{N03A} = 2.3E-6

(LCI-21): Check Valve VCM-30AN-42A, fails to open on demand, P_{F42A}= 1.1E-6

(LCI-22): Relay 10A-K19A, fails to remain open, P_{FRO} = 6.9E-7

(LCI-23): Valve P-3A, fails to close (plugged), P_{FPGP3A} = 2.0E-7

(LCI-23): Valve MOV65A fails to close (plugged), P_{FPG65A} = 2.0E-7

(LCI-25): Valve MOV12A, fails to close (plugged), P_{FPG12A} = 2.0E-7

(LCI-26): Manual Valve 151A, fails to close (plugged), P_{PG151A} = 1.6E-7

Table 4.4 - Plant Risk Contributions from Basic Events (Page 3 of 4)

Emergency Service Water System (ESW)

(ESW-1): Loop B, unavailable due to maintenace, P_{MLPB} = 2.8E-6

(ESW-2): Loop A, unavailable due to maintenace, P_{MLPA} = 1.9E-6

(ESW-3): Motor Driven Pump 46-2A, fails to remain running, P_{FRA}= 2.2E-6

(ESW-4): Motor Driven Pump 46-2B, fails to remain running, P_{FRB}= 2.2E-6

(ESW-5): Manual Valve 3B, fail to restore after test, P_{FR3B} = 5.7E-7

(ESW-6): Manual Valve 3A, fail to restore after test, P_{FR3A} = 5.7E-7

AC Power System (AC4)

(AC4-1): Bus 10600 UV Relay, miscalibration, P_{MC} = 5.7E-7

(AC4-2): Bus 10500 UV Relay, miscalibration, P_{MC} = 5.7E-7

(AC4-3): Lower Relay 86A-1HOEB03 Path, fails, $P_{RL86FB3}$= 8.8E-7

(AC4-4): Lower Relay 86A-1HOEB01 Path, fails, $P_{RL86FB1}$= 8.8E-7

(AC4-5): Lower Relay 86A-1HOEA01 Path, fails, $P_{RL86FA1}$ = 1.9E-8

(AC4-6): Circuit Breaker 10640, fails normally running, P_{FNR1}= 1.5E-6

(AC4-7): Circuit Breaker 10550, fails normally running, P_{FNR2} = 1.5E-6

High Pressure Coolant Injection System (HCI)

(HCI-1): System, unavailable due to maintenance, P_{HCIMA} = 2.9E-7

(HCI-2): Turbine Driven Pump, fails to run, P_{PFR} = 4.2E-8

(HCI-3): Turbine Driven Pump, fails to start, P_{PFR} = 4.8E-8

(HCI-4): Steam Supply/Exhaust Path, fails, P_{SUPF} = 1.7E-8

DC Power System (DC1)

(DC1-1): BCB-2B Panel, fault, by any load, P_{PLF2B}= 1.7E-8

(DC1-2): 10500 Panel, fault, by any load, $P_{PLF10500}$ = 1.3E-7

(DC1-3): 10600 Panel, fault, by any load, $P_{PLF10600}$ = 1.3E-7

(DC1-4): 71DC-A4, fault, by any load, P_{PLF-A4} = 1.3E-7

(DC1-5): BCB-2A Panel, fault, by any load, P_{PLF2A} = 1.3E-7

(DC1-6): DC Fuse, blown (negative), P_{FBL}= 9.8E-8

Table 4.4 - Plant Risk Contributions from Basic Events (Page 4 of 4)

Turbine Building Closed Cooling Water System (TBC)

(TBC-1): Control Circuit for Pump 37P-2B, fails, P_{PCF} = 1.0E-9

(TBC-2): Control Circuit for Pump 37P-2A, fails, P_{PCF} = 1.0E-9

(TBC-3): Pump 37P-2B, unavailable due to maintenance, P_{PMF} = 8.8E-10

(TBC-4): Pump 37P-2B, fails to restore after maintenance, P_{FR} = 2.1E-10

AC Power System (ACO)

(ACO-1): Transformer T3, unavailable due to maintenance, P_{T3U} = 1.6E-9

(ACO-2): Transformer T2, unavailable due to maintenance, P_{T2U} = 1.6E-9

Suppression Pool Cooling (SPC)

(SPC-1): Service Water 10A-S17A path, fault, P_{F-S17A} = 5.5E-7

Table 4.5 - System Importance Rankings

System	Ranking
LPCI	1
RSW	2
ESW	3
AC4	4
DC1	5
SPC	6
HPCI	7
TBC	8
ACO	9

Table 4.6 - Component Group Ranking

GROUP	RANKING
PUMPS	1
VALVES	2
HEAT EXCHANGERS	3
CONTROL CIRCUITS	4
TRAINS	5
RELAYS	6
SWITCHGEAR	7
BUSES	8
FUSES	9
TRANSFORMERS	10

Table 4.7 - LPCI System Component Importance Ranking

COMPONENT & FAILURE MODES	FAILURE DATA	RANKING
4 RHR Pumps — FS	2.8E-5	1
PM-3A Path — RE	2.2E-5	2
PM-3D Path — RE	2.1E-5	3
Heat Exchanger E-2A — DN E-2b — DN	1.2E-5	4
Check valve VCM-30AN-42B → CO VCM-30AN-42C → CO	6.9E-6	5
Control Circuit RP-3A → NO	2.3E-6	6
Check valve VCM-30AN-42A → CC VCM-30AN-42D → CC	1.1E-6	7
Relay 10A-K19 → C	6.9E-7	8
Relay 10A-K22B → OC	5.9E-7	9
Control Circuit RP-3D → NO	2.3E-7	10
MOV12B → PG MOV65B → PG Valve P-3A → PG MOV65A → PG MOV12A → PG	2.0E-7	11
Valve VCM-30AN-45D → PG Manual valve 151A →PG	1.6E-7	12
MOV 16A → CC 16B → CC	1.3E-8	13
Relay 10A-K48A path → NO 10A-K48B Path → NO	4.5E-9	14
Pump P-3D → FR	2.6E-10	15
Switchgear 10-S3D → DN	1.2E-10	16

Table 4.8 - Importance Matrix

INSIDE MODES RANKINGS GLOBAL RANKING FAILURE CAUSES	COMPONENT FAILURE MODES											
	CC	OC	CO	PG	FS	FR	ST	NO	DN	MC	RE	MA
*** VALVES ***			Valve Group Ranking = 2									
RSW SYSTEM		1										
2 DISCH. MOVS		1										
RSW SYSTEM		3										
MOV 89A			16									
RSW SYSTEM		3										
MOV 89B			16									
RSW SYSTEM					2							
MANU VALVE 24B					24							
RSW SYSTEM					2							
MANU.VALVE 11B					24							
LPCI SYSTEM		4										
MOV 16A		31										
LPCI SYSTEM		4										
MOV 16B		31										
LPCI SYSTEM		2										
CHK. VALVE 42A		14										
LPCI SYSTEM		1										
CHK. VALVE 42B		8										
LPCI SYSTEM		1										
CHK. VALVE 42C		8										
LPCI SYSTEM		2										
CHK. VALVE 42D		14										
LPCI SYSTEM		1										
MOV 12B		23										
LPCI SYSTEM				1								
MOV 65B				23								
LPCI SYSTEM				2								
CHK. VALCE 45D				24								

	CC	OC	CO	PG	FS	FR	ST	NO	DN	MC	RE	MA
LPCI SYSTEM				1								
MOV 3A				23								
LPCI SYSTEM				1								
MOV 65A				23								
LPCI SYSTEM				1								
MOV 12A				23								
LPCI SYSTEM				2								
MA.VALVE 151A				24								
ESW SYSTEM						2						
MANU. VALVE 3A						19						
ESW SYSTEM						2						
MANU. VALVE 3B						19						
*** PUMPS ***			Pump Group Ranking = 1									
RSW SYSTEM					2	3						
PUMP 1A					6	24						
RSW SYSTEM					2							
PUMP 1B					6							
RSW SYSTEM					2							4
PUMP 1C					6							24
RSW SYSTEM					2							
PUMP 1D					6							
LPCI SYSTEM					1							1
PUMP 3A					2							3
LPCI SYSTEM					1							
PUMP 3B					2							
LPCI SYSTEM					1							
PUMP 3C					2							
LPCI SYSTEM					1	5						2
PUMP 3D					2	37						4
ESW SYSTEM						1						
PUMP 2A						11						
ESW SYSTEM						1						
PUMP 2B						11						

* PUMPS * (cont.)	CC	OC	CO	PG	FS	FR	ST	NO	DN	MC	RE	MA
HPCI SYSTEM					3	4						
TUB. DIV. PUMP					27	28						
TBC SYSTEM											3	5
PUMP 37P-2B											38	36

*** CON. CIRCUITS *** Control Circuit Group Ranking = 4

	CC	OC	CO	PG	FS	FR	ST	NO	DN	MC	RE	MA
RSW SYSTEM								1				
MOV 89A CON.								7				
RSW SYSTEM								1				
MOV 89B CON.								7				
LPCI SYSTEM								2				
SWG.CON.RP-3A								10				
LPCI SYSTEM								4				
SWG.CON.RP-3D								22				
AC4 SYSTEM									2			
BREAKER 10640									13			
AC4 SYSTEM									2			
BREAKER 10550									13			
TBC SYSTEM								9				
P37-2A CONTROL								35				
TBC SYSTEM								9				
P37-2B CONTROL								35				

	CC	OC	CO	PG	FS	FR	ST	NO	DN	MC	RE	MA
* **RELAYS** *			Relay Group Ranking = 6									
LPCI SYSTEM 10A-K48A PATH								7 32				
LPCI SYSTEM 10A-K48B PATH								8 33				
LPCI SYSTEM 10A-K22B PATH		1 18										
LPCI SYSTEM 10A-K19A PATH			2 17									
AC4 SYSTEM 10600 BUS UV									1 19			
AC4 SYSTEM 10500 BUS UV									1 19			
AC4 SYSTEM 86A-1HOEA01								6 29				
AC4 SYSTEM 86A-1HOEB01								3 15				
AC4-SYSTEM 86A-1HOEB03								3 15				
* **ELEC BUSES** *			Buses Group Ranking = 8									
DC1 SYSTEM BCB-2A							1 25					
DC1 SYSTEM BCB-2B							2 30					
DC1 SYSTEM 10500 PANEL							1 25					
DC1 SYSTEM 10600 PANEL							1 25					
DC1 SYSTEM 71DC-A4 DIV							1 25					

	CC	OC	CO	PG	FS	FR	ST	NO	DN	MC	RE	MA
* **SWITCHGEAR** * Switchgear Group Ranking = 7												
RSW SYSTEM 10A-S48B PATH								3 20				
RSW SYSTEM 10A-S48A PATH								3 20				
SPC SYSTEM 10A-S17A PATH								3 20				
LPCI SYSTEM SWG. 10-S3D								5 39				
* **HEAT EXCHANGER** * Heat Exchanger Group Ranking = 3												
LPCI SYSTEM LOOP A-E2A									1 5			
LPCI SYSTEM LOOP B-E2B									1 5			
* **TRAINS** * Trains Group Ranking = 5												
ESW SYSTEM LOOP A												2 12
ESW SYSTEM LOOP B												1 9
HPCI SYSTEM STEAM SUP. PATH									4 30			
HPCI SYSTEM WHOLE SYSTEM												3 21
* **TRANSFORMER** * Transformer Group Ranking = 10												
ACO SYSTEM TRANSFORMER 2												4 34
ACO SYSTEM TRANSFORMER 3												4 34
* **FUSES** * Fuse Group Ranking = 9												
DC1 SYSTEM DC FUSE									5 26			

The Failure Modes, as defined in JAF PRA analysis, are listed below:

CC	Normally closed, fails to open on demand
OC	Normally open, fails to remain open
CO	Normally closed, fails to remain closed
PG	Plugged, blockage
FS	Fails to start
FR	Fails to continue running
ST	Short circuit
NO	No output
DN	Does not operate
MC	Miscalibration
RE	Failure to restore to correct position following test and maintenance
MA	Unavailable due to maintenance

The Failure Causes are defined as follow:

CCF	Common Cause Failure
TE	Test
MAI	Maintenance

Table 4.9 - Loss of Containment Heat Removal Initiator Frequencies Before Recovery

Initiator		Frequency*
T1		2.03E-5/RY
T2		7.05E-5/RY
T3A		4.95E-6/RY
T3B		1.43E-6/RY
T3C		3.50E-7/RY
TAC-10500		1.60E-6/RY
TAC-10600		5.00E-8/RY
TDC-A		3.90E-5/RY
TDC-B		3.95E-5/RY
A		1.76E-8/RY
S1		7.23E-8/RY
S2		2.24E-8/RY
	Total	1.69E-4/RY

*Each frequency is calculated by summing the individual sequence frequencies that are dominant (i.e., >1.0E-9)

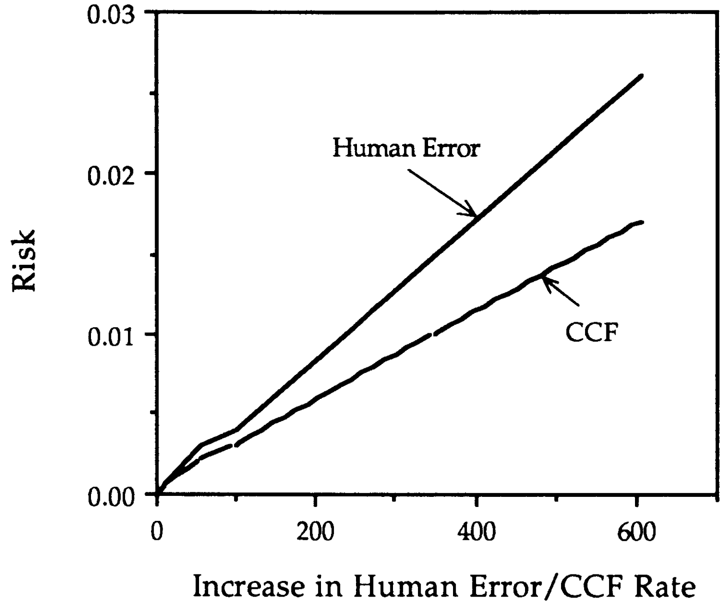


Figure 4.1 - Scoping Calculation (Change in Risk With Change in Human Error and CCF Rates)

5. MAINTENANCE PROGRAM IMPACT ON CCF RATES

In Section 4.2.2, 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[10]. CCF events have been found to be dominant risk contributors in many PRA studies. This section develops an approach for analyzing the effects of different maintenance practices on the likelihood of common cause failure, and applies this approach to a number of test cases. The approach is used to analyze postulated changes in the JAF maintenance program in Section 7.

5.1 General Procedure for Calculating CCF Rates

Ref. 37 presents a general approach for including common cause failures in a PRA study. (As noted in earlier sections, "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, and 4) system quantification and interpretation of results. This work focuses on the third stage, since the results of the first two stages are incorporated in the JAF IPE, and the fourth stage is the subject of Section 7 of this report.

According to Ref. 37, 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 common cause failure model parameters.

The following subsections discuss the application of these steps towards the analysis of the failure of 4 RHR pumps.

5.1.1 Step 1 – Common Cause Basic Event Definition

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,...,m) fail due to a single cause.

In this study, the basic event of interest is the common cause failure of 4 motor–driven RHR pumps. This frequency of this event is denoted by Q_{4mdp} in the remainder of this study.

5.1.2 Step 2 – Selection of Probability Model

A number of probability models for CCF analysis are presented in Ref. 37. In particular, it describes both the β–factor model [38], which is used in the JAF IPE, and an improved version, the α–factor model [9], which is used in this study. As discussed in Refs. 9 and 37, the α–factor model has two advantages: a) it explicitly treats different

[10] The basic event is denoted LCI–CCF–PF–4MDPM in the James A. Fitzpatrick (JAF) Individual Plant Examination (IPE).

levels of common cause failure events, and b) uncertainties in 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 frequency of interest, Q_{4mdp}, is computed as follows:

$$Q_{4mdp} = \frac{4\alpha_4\phi_d}{\alpha_t} \tag{5.1}$$

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, due to their low likelihood)
$\alpha_t \equiv$ a normalization factor, $\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4$.

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.

5.1.3 Step 3 – CCF Event Data Classification and Screening

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. 37 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 5.2 discusses the performance of this task for the RHR pump CCF data.

5.1.4 Step 4 – CCF Parameter Estimation

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

$$\hat{\alpha}_k = \frac{n_k}{\sum_{i=1}^{m} n_i} \tag{5.2}$$

where m is the number of components in the common cause group. However, in practice, there may be significant uncertainty in the n_k [37,39].

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 by the common cause 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 [37]:

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

$$\mathbf{q}_j = \{q_{0j}, q_{1j}, \cdots, q_{kj}, \cdots, q_{mj}\} \tag{5.3}$$

where q_{kj} is the probability that the jth event involved the common cause failure of k components. If the impact of the event is known with certainty, one p_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 pump failed to start on demand because of a 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. 37 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:

$$p_j = \{p_{0j}, p_{1j}, \cdots, p_{kj}, \cdots, p_{mj}\} \tag{5.4}$$

where p_{kj} is the probability that the jth 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[11]:

$$\hat{\alpha}_k = \frac{\bar{n}_k}{\sum\limits_{i=1}^{m} \bar{n}_i} \tag{5.5}$$

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,

$$\bar{n}_k = \sum_{j=1}^{N} p_{kj} \tag{5.6}$$

The application of this estimation procedure in the analysis of RHR pump common cause failures is discussed in Section 5.3.

5.2 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 JAF. The screening is based on the rules provided in Section 5.1.3, 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 linking mechanisms underlying each of the multiple failure events in the screened data base.

5.2.1 Data Sources

Ref. 40 provides an analysis of RHR pump failure events occurring over the period 1972 through 1981. Ref. 41 summarizes RHR pump failure events for the period 1972 through 1980. Ref. 41 provides more information on system performance and failure causes, and is used as the basis for the quantitative analysis done in this study.

5.2.2 Selection of Events

Ref. 41 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:

[11] This use of the average values for the n_k is approximate. Ref. 39 provides an exact approach for dealing with data uncertainties, but also shows that the error in the point estimate for α_k generated using the approximate method is usually small.

- 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. 41, "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 separately).

- Only "fail to start" events are included. Runtime failures, although observed, do not contribute significantly to plant risk.

Table 5.1 provides a listing of the 17 events surviving the screening process. Table 5.2 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 5.3 provides the failure codes used in Table 5.1.

5.2.3 RHR Pump Failure Mechanisms

Some understanding of the failure mechanisms underlying the RHR pump failure events in Table 5.1 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.

5.2.3.1 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 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. 42.

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 5.4, could be a deficiency in the maintenance program. If so, then this deficiency is the root cause of the event.

Ref. 42 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 5.1 are presented in Table 5.5. These are later used when assessing the CCF event impact vectors.

5.2.3.2 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 [37,42]. 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 5.1 are presented in Table 5.6. These are later used when assessing the CCF event impact vectors.

5.3 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 5.1. The approach is applied to the JAF maintenance program and postulated changes in that program in Section 7.

5.3.1 Initial Impact Vectors for Actual Events

As stated in Section 5.1.4, 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. 37, as discussed in Section 5.4.3.

  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

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

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

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

- The impact vectors for each event [see Eq. (5.3)]. 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 5.1 are presented in Table 5.7.

5.3.2 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, in principle, 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_{ki}) are different from the initial impact vector profiles (the relative values of the q_{ki}). This section discusses the applicability assessment. The mapping up/down procedure is briefly discussed in Section 5.3.3. 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 CCF event, the procedure results in a probability that the event's root cause is applicable to the new system, and a probability that the event's coupling mechanism is applicable to the new system. Define the "root cause applicability" and the "coupling mechanism applicability" as follows:

$$a_{rcj} = P\{\text{root cause for Event j is applicable to plant}\}$$
$$a_{cmj} = P\{\text{coupling mechanism for Event j is applicable to plant}\}$$

Treating the root cause and coupling mechanisms as being independent (this assumption can be relaxed on a case–by–case basis), the overall applicability of Event j is then defined as

$$a_j \equiv a_{rcj} * a_{cmj} \tag{5.7}$$

(Note that when Event j does not involve multiple failures, $a_{cmj} = 1$.) This is the probability that the event is applicable and should be used in the estimation of α–factors. Using a_j, the average impact vector for Event j is then obtained using the definition of conditional probability:

$$\begin{aligned} \mathbf{p}_j \; = \; & a_j * \mathbf{p}_j(\text{given that Event j is applicable}) \\ & + (1 - a_j) * \mathbf{p}_j(\text{given that Event j is not applicable}) \end{aligned} \tag{5.8}$$

For example, consider Event 9 in Table 5.1. The plant experiencing this event has 3 RHR pumps. The original impact vector assessed for this event is

$$\mathbf{q}_9 = (0, 0.8, 0.1, 0.1)$$

If the plant being analyzed also has 3 RHR pumps, the modified impact vector suitable for use in estimating α_1, α_2, and α_3 is:

$$\mathbf{p}_9 = (1 - a_9, 0.8a_9, 0.1a_9, 0.1a_9)$$

If the plant being analyzed has more than 3 RHR pumps, this impact vector must be modified using the "mapping up" procedure described in Ref. 37.

The root cause and coupling mechanism applicabilities a_{rcj} and a_{cmj} 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 5.5 and 5.6.

The quantitative effects of the root cause defenses (expressed at the level of the maintenance program block diagram shown in Figure 2.1) are determined using Table 5.8.

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 again 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 5.9–5.12) should be used in the root cause portion of the applicability analysis; their use is described below. The entries in Tables 5.9–5.12 are based on failure rate multipliers collected from a variety of sources. 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 5.13. 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 again conditioning events that will allow the coupling mechanism to link multiple failures. The entries in the matrix indicate which of Tables 5.14–5.17 should be used in the coupling mechanism portion of the applicability analysis; their use is described below. The entries in Tables 5.14–5.17 are also based on failure rate multipliers collected from a variety of sources. It is assumed that these failure rate multipliers can be used directly in an applicability assessment.

In general, the root cause applicability is a function of the failure rate multipliers provided in Tables 5.9–5.12. Assuming that a simple linear combination model is reasonable,

$$a_{rcj} = \sum_k w_{rc,k} M_{rc\text{-}md,k} \tag{5.9}$$

where the summation is over the different contributing root causes for event j, $M_{rc\text{-}md,k}$ is a multiplier for root cause k (given the maintenance defenses for the plant experiencing the event and the defenses for the plant being analyzed) derived from the values presented in Tables 5.9–5.12, and $w_{rc,k}$ is the assigned weight used to reflect which root cause is dominant. The coupling mechanism applicability, a_{cmj}, is computed similarly.

The following procedure is used to apply Eq. (5.9).

<u>Step 1</u>

General: Develop the root cause weights (w_{rc}) for each event. Assuming that one of the root causes is dominant, the following three rules are used to assign weights:

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

Note that if an event involves more contributing root causes, these rules may need to be extended.

Example: For Event 9, assume that a lack of RHR pump–specific training and complete reliance on corrective maintenance are the two root causes. Let the latter be the dominant one. Then the root cause weights are:

$$w_{rc}(\text{training}) = 0.2$$
$$w_{rc}(\text{maintenance policy}) = 0.8$$

Step 2

General: Develop the coupling mechanism weights (w_{cm}) for each event. 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 any staggerring in schedule). Assuming that the latter is dominant, we have:

$$w_{cm}(\text{procedure}) = 0.2$$
$$w_{cm}(\text{crew}) = 0.8$$

Step 3

General: For each contributing root cause and each conditioning event defense, assess the appropriate RC–MD multiplier (this is a function of the current practice for each maintenance program block). 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/conditioning event 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 1 above. 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 2 above). The product of the average RC–MD multiplier and the average CM–MD multiplier is the applicability for the event.

Example: Continue with Event 9. 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 5.8 is 'm2'; this indicates that Table 5.10 is used to provide the multiplier value.

$$M_{rc\text{-}md}(\text{training}) = \frac{0.95}{1.2} = 0.79$$

Assume that at the plant being analyzed, only corrective maintenance is used. The relevant entry in Table 5.8 is 'm3'; this indicates that Table 5.11 is used to provide the multiplier value.

$$M_{rc\text{-}md}(\text{maintenance policy}) = \frac{1.3}{1.3} = 1.0$$

The average applicability for the contributing root causes is then given by

$$\begin{aligned} a_{rc9} &= w_{rc}(\text{training})*M_{rc\text{-md}}(\text{training}) + \\ &\qquad w_{rc}(\text{maintenance policy})*M_{rc\text{-md}}(\text{maintenance policy}) \\ &= 0.2*0.79 + 0.8*1.0 \\ &= 0.96 \end{aligned}$$

The average applicability for the contributing coupling mechanisms is found in a similar manner. Assuming that at the plant being analyzed, the same crew performs the maintenance actions on both pumps but the maintenance is staggered, the relevant entries in Table 5.13 are 'm5' and 'm6'. Assuming that the procedures at the plant being analyzed are also deficient, the relevant entry is 'm8'. Using Tables 5.14, 5.15, and 5.17, there obtains

$$M_{cm\text{-md}}(\text{crew}) = \frac{0.5}{1.0}*\frac{0.2}{0.2} = 0.5$$

$$M_{cm\text{-md}}(\text{procedures}) = \frac{0.5}{0.5} = 1.0$$

Thus

$$\begin{aligned} a_{cm9} &= w_{cm}(\text{crew})*M_{cm\text{-md}}(\text{crew}) + w_{cm}(\text{procedures})*M_{cm\text{-md}}(\text{procedures}) \\ &= 0.8*0.5 + 0.2*1.0 \\ &= 0.6 \end{aligned}$$

The total applicability for Event 9 is then given by

$$a_9 = a_{rc9}*a_{cm9} = 0.58$$

The modified impact vector for Event 9 is then

$$\mathbf{p}_9 = (0.42, 0.46, 0.06, 0.06)$$

Note that this impact vector may need to be modified to account for 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 used in this section is only applied to a single plant maintenance program. It can be seen that the same approach can be used to determine the impact of maintenance programs changes on event applicability. The applicability quantification procedure described above is illustrated in Figure 5.2.

5.3.3 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.

Consider for example, Event 9 in Table 5.1. As mentioned previously, this event occurred at a plant with only 3 RHR pumps. The modified impact vector assessed for this plant, $\mathbf{p}_9 = (1 - a_9, 0.8a_9, 0.1a_9, 0.1a_9)$ is not necessarily directly applicable to a plant with 4 RHR pumps.

To account for differences in system (or more precisely, common cause component group) size, Ref. 37 provides "mapping up" and "mapping down" procedures. These procedures are summarized in Tables 5.18 and 5.19; it can be seen that the parameter ρ assessed earlier in Section 5.3.1 is needed at this point.

To illustrate the use of these tables, assume that the modified impact vector for Event 9 is to be mapped up to a plant with 4 RHR pumps. Let the non–lethal shock probability (ρ) be 0.50. Using the equations in Table 5.18 for the 3 → 4 mapping, we obtain the following final impact vector:

$$\mathbf{p}_9 = (0.34, 0.31, 0.26, 0.06, 0.03)$$

The impact vectors for RHR pump failures, modified to account for applicability and system size, are presented in Table 5.20. These are used in the estimation of the α–factor model parameters, as described in the following section.

5.3.4 Estimation of CCF Parameters

Given the impact vectors in Table 5.20, the α–factors can be estimated in a straightforward fashion using Eqs. (5.5) and (5.6). Note that the data provided by Ref. 41 can also be useful for estimating ϕ_d. For a 4–pump system,

$$\hat{\phi}_d = \frac{1}{4N_d} \sum_{k=1}^{4} k*\bar{n}_k \tag{5.10}$$

In order to reflect the impact of changes in maintenance on ϕ_d, the maximum likelihood estimator is modified as follows:

$$\phi_d = \hat{\phi}_d \prod_i \frac{M_{rc\text{-}md,i}(\text{modified program})}{M_{rc\text{-}md,i}(\text{baseline program})} \prod_j \frac{M_{cm\text{-}md,j}(\text{modified program})}{M_{cm\text{-}md,j}(\text{baseline program})} \tag{5.11}$$

This equation is used in the sensitivity analyses presented in Section 7.

Using Eqs. (5.2) and (5.10), the following maximum–likelihood estimates for the α–factor model parameters are obtained using root cause and coupling mechanism weights/multipliers that best characterize the JAF maintenance program:

$$\hat{\alpha}_1 = 0.76$$
$$\hat{\alpha}_2 = 0.18$$
$$\hat{\alpha}_3 = 0.05$$
$$\hat{\alpha}_4 = 0.01$$
$$\hat{\phi}_d = 0.005/\text{demand}$$

Using Eq. (5.1), a point estimate for Q_{4mdp} is found:

$$\hat{Q}_{4mdp} = 1.6*10^{-4}$$

Table 5.1 – 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 torus WTR. TEMP.	Dirty switch in 4kv for pump
10	DR2	041579	B00, , U	2A LPCI pump would not start	Cause unknown

Table 5.1 – 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 current

Table 5.2 – 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
OE1	Oconee 1	3	89	22540
CC1	Calvert Cliffs 1	2	72	19225
CC2	Calvert Cliffs 2	2	46	13405
MI2	Millstone 2	2	60	15290
BF3	Browns Ferry 3	4	50	13481
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
NM1	Nine Mile Point 1	3	105	29283
PB2	Peach Bottom 2	4	85	20249
PB3	Peach Bottom 3	4	74	20137
VY1	Vermont Yankee	4	102	28713
BV1	Beaver Valley	2	52	6888
DC2	D.C. Coole 2	2	30	8406
HN1	Haddam Neck	2	105	31753
SA1	Salem 1	2	46	8244
SU1	Surry 1	2	99	21260
TR1	Trojan	2	57	10999
YR1	Yankee Rowe	3	105	26758

Table 5.3 – Failure Codes Used in Table 5.1

Failure Code

	Failure Mode		Failure Cause
CODE	DESCRIPTION	CODE	DECRIPTION
A —	leakage / rupture	00 —	unknown
B —	does not start	01 —	personnel (operations)
C —	losS of function	02 —	personnel (maintenance)
D —	does not continue to run	03 —	personnel (testing)
		04 —	design errors
		05 —	fab./construction/q.c
		06 —	procedural discrepances
		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	D —	demand
C —	common cause failures	T —	time
R —	recurring failures	U —	unknown
S —	command faults		
T —	recurring command faults		
U —	common cause command faults		
V —	recurring common cause command faults		

Table 5.4 – Proximate Cause of Event 38 (Lack of Lubrication)

Immediate Cause/Reason	Effect/Problem
Motor bursting into flames	Pump stops running
Insufficient lubrication to LWR RAD.BRNG	Motor bursting into flames
Failure to perform preventive maintenance	Insufficient lubrication to LWR RAD.BRNG.
Foreman forgot to do it	Failure to perform preventive maintenance
Foreman did not perform job properly	Failure to perform preventive maintenance
Programmatic deficiency: there is no formal scheduling system to plant preventive maintenance activities; or procedure was not double–checked	Foreman forgot to do it
There is no training provided on lubrication job	Foreman did not perform the job properly

Table 5.5 - Root Causes 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 of personnel
3	BR1	Environmental contamination on control switch	Only corrective maintenance (d); no training of personnel
4	BR1	Pump cover corroded due to leaking	Only corrective maintenance (d); no training of personnel
5	BR1	Circuit breaker internal failure	Procedure bad; personnel not trained; only CM (d)
6	BR2	Fuse poorly connected	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	Environmental contamination on control switch	Only corrective maintenance (d); no training of personnel
10	DR2	No obvious evidence observed	All three possible root causes as in Event Number 1
11	EN1	Circuit breaker internal failure	Procedure bad; personnel not trained; only CM (d)
12	EN2	Relay wire missing	Procedure bad; personnel not trained (d)
13	FP1	Circuit breaker internal failure	Only corrective maintenance (d); no training of 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	Sequential contact open due to low CRNT	Procedure bad; only corrective maintenance (d)

Table 5.6 - 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	Environmental contamination on control switch	
4	BR1	Pump cover corroded due to leaking	Procedure training (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	Environmental contamination on control switch	Staff scheduling (d); same deficient procedure used
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 used
15	PB2	Pump disabled by human error	Staff scheduling (d); same deficient procedure used
16	VY1	Circuit breaker poorly connected	
17	TR1	Sequential contact open due to low CRNT	Deficient procedure used (d)

Note: (d) = dominant

Table 5.7 - 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

Table 5.8 - Root Cause/Maintenance Defense Matrix

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				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 of breakers				m1	m2	m3	
Control switch disabled by human error						m3	m4
Control switch internal failures				m1	m2	m3	
Environmental contamination of control switch				m1	m2	m3	
Relay internal failure				m1	m2	m3	
Pump disabled by human error						m3	m4

Note: The empty entries mean that defenses are not available. Qualitatively they indicate that those modifiers are equal to one.

Table 5.9: Modifier 'm1' to Account for the Impact of Maintenance Quality on Electrical Equipment Failure Rate (ANSI/IEEE Std. 493-1980)

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 5.10: Modifier 'm2' to Account for the Impact of Training on Quality of Electrical/Mechanical Component Failure Rate

Quality of Training	Failure Rate Modifier
	Electrical/Mechanical Component
Trained in Specific Procedure	0.95
Not Trained in Specific Procedure	1.2

Table 5.11: Modifier 'm3' to Account for the Impact of Training Levels on Electrical/Mechanical Component Failure Rate

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

Table 5.12: Modifier 'm4' for the Impact of Procedure Quality

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 5.13: Coupling Mechanisms - Maintenance Defense Matrix

Failure Mechanisms	Selected Defense Against the Conditioning Events						
	BLOCK 1			BLOCK 2	BLOCK 8		
	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 Installed	m5	m6	m7				m8
Breaker Internal Failures	m5	m6					m8
Breaker with Poor Connection	m5	m6					m8
Environmental Contamination of Breakers	m5	m6					m8
Control Switch Disabled by Human Error	m5	m6	m7				m8
Control Switch Internal Failures	m5	m6					m8
Environmental Contamination of Control Switch	m5	m6					m8
Relay Internal Failure	m5	m6					m8
Pump Disabled by Human Errors	m5	m6	m7				m8

Note: The empty entries mean that defenses are not available.
Qualitatively they mean that these modifiers are equal to 1.

Table 5.14: Modifier 'm5' for the Impact of Maintenance Scheduling

Maintenance Schduling	Coupling Mechanisms Modifier
	All Components
Staggered on Trains	0.25
Staggered on Loops	0.5
Non-staggered	1

Table 5.15: Modifier 'm6' for the Impact of Staff Diversity Effect

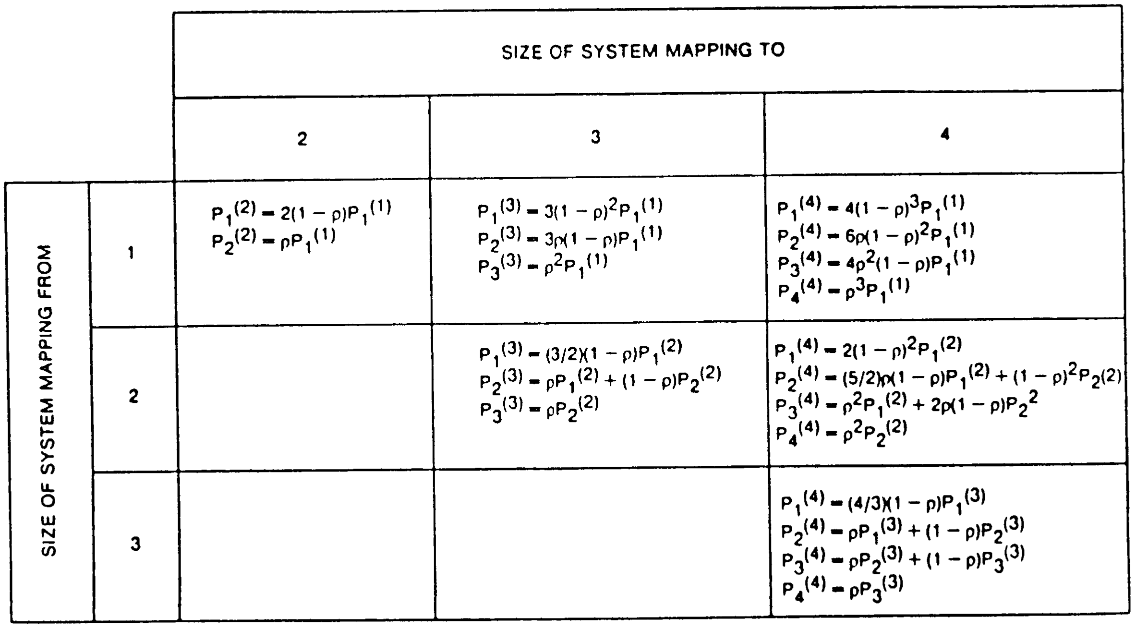
Staff Diversity	Coupling Mechanisms Modifier
	All Components
Different in Each Train	0.05
Different in Each Loop	0.1
Diversity not Implemented	0.2

Table 5.16: Modifier 'm7' for the Impact of Staff Area Allocation

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

Table 5.17: Modifier 'm8' for the Impact of Procedure Quality On Coupling Mechanisms:

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



		SIZE OF SYSTEM MAPPING TO		
		2	3	4
SIZE OF SYSTEM MAPPING FROM	1	$P_1^{(2)} = 2(1-\rho)P_1^{(1)}$ $P_2^{(2)} = \rho P_1^{(1)}$	$P_1^{(3)} = 3(1-\rho)^2P_1^{(1)}$ $P_2^{(3)} = 3\rho(1-\rho)P_1^{(1)}$ $P_3^{(3)} = \rho^2P_1^{(1)}$	$P_1^{(4)} = 4(1-\rho)^3P_1^{(1)}$ $P_2^{(4)} = 6\rho(1-\rho)^2P_1^{(1)}$ $P_3^{(4)} = 4\rho^2(1-\rho)P_1^{(1)}$ $P_4^{(4)} = \rho^3P_1^{(1)}$
	2		$P_1^{(3)} = (3/2)(1-\rho)P_1^{(2)}$ $P_2^{(3)} = \rho P_1^{(2)} + (1-\rho)P_2^{(2)}$ $P_3^{(3)} = \rho P_2^{(2)}$	$P_1^{(4)} = 2(1-\rho)^2P_1^{(2)}$ $P_2^{(4)} = (5/2)\rho(1-\rho)P_1^{(2)} + (1-\rho)^2P_{2(2)}$ $P_3^{(4)} = \rho^2P_1^{(2)} + 2\rho(1-\rho)P_2^2$ $P_4^{(4)} = \rho^2P_2^{(2)}$
	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 5.18 - Mapping Up Procedure
(from NUREG/CR-4780, Vol. 2, p. D-16)

		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 5.19 - Mapping Down Procedure
(from NUREG/CR-4780, Vol. 2, p. D-9)

Table 5.20 - Baseline Case Event Impact Vectors After Applicability and System Size Mappings

Event Number		P_0	P_1	P_2	P_3	P_4	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		0.6
	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	9		
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	0.958	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	0.8	0.2	0	0		0.958	0.6
	JAF Plant	0.425	0.429	0.178	0.058	0.017		
10	Actual Plant	0	1	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		
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	1	0			1	
	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**		

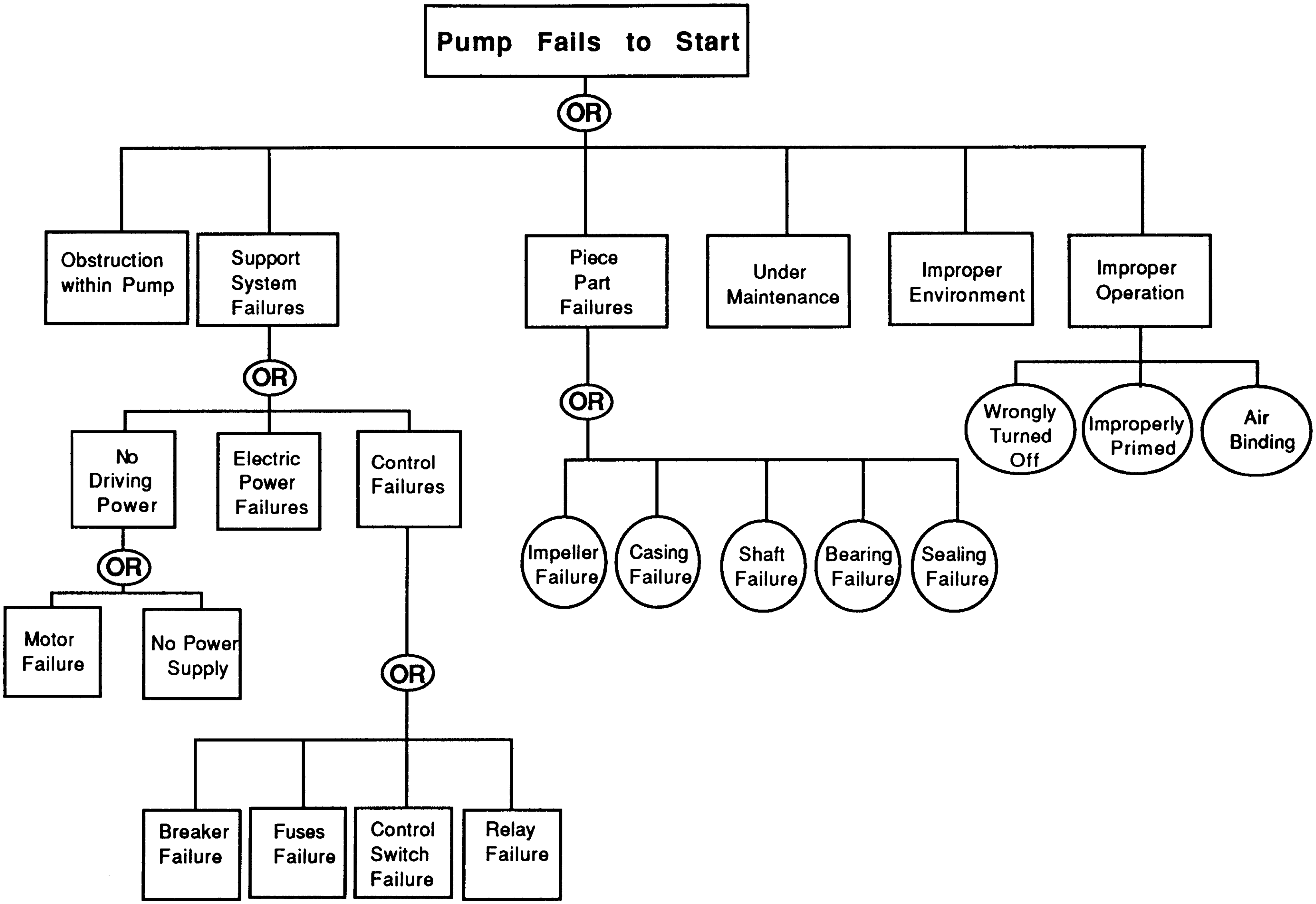
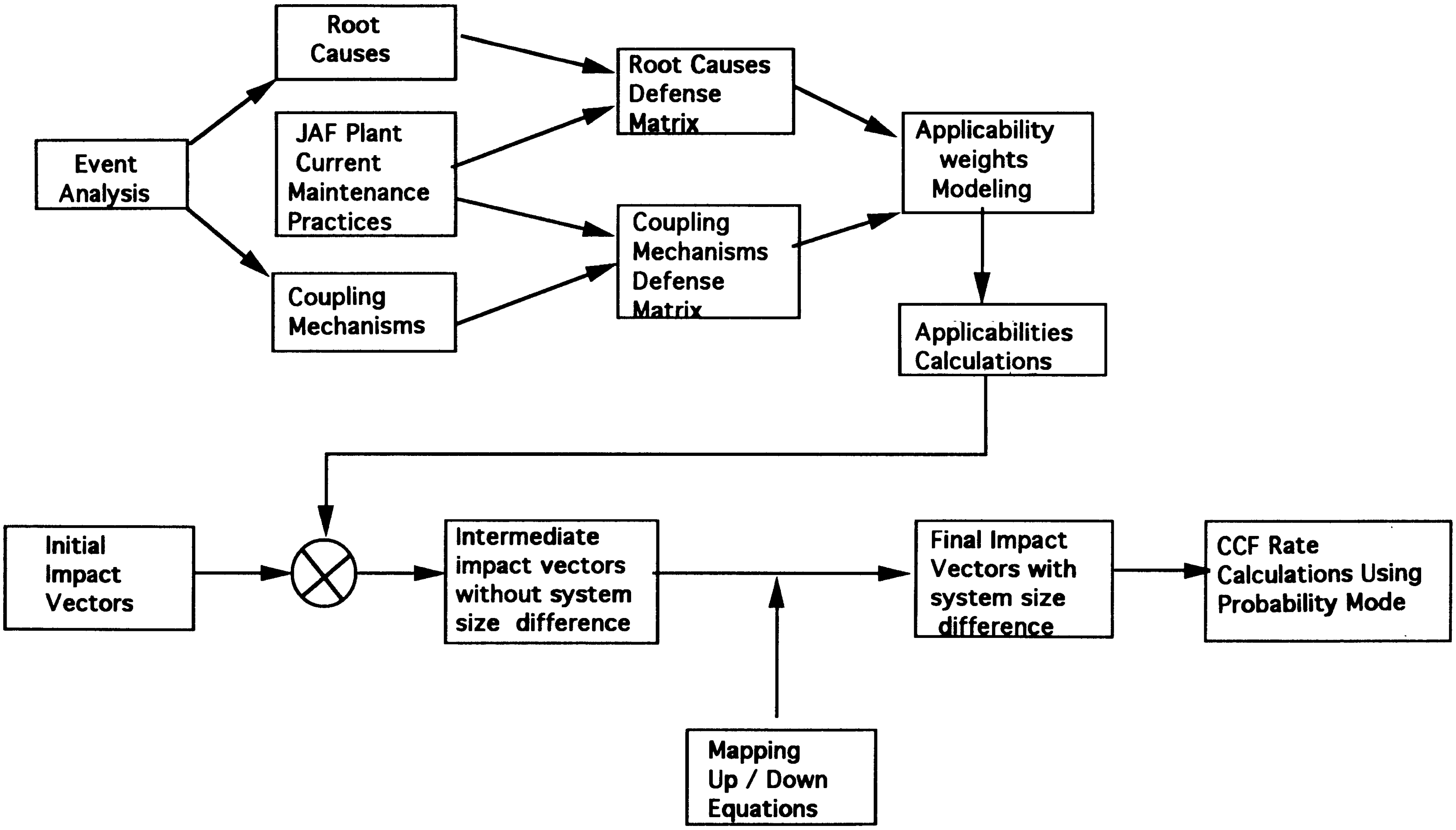


Fig. 5.1 - RHR Pump 'FS' Mode Failure Mechanisms


Event Analysis
Root Causes
JAF Plant Current Maintenance Practices
Coupling Mechanisms
Root Causes Defense Matrix
Coupling Mechanisms Defense Matrix
Applicability weights Modeling
Applicabilities Calculations
Initial Impact Vectors
Intermediate impact vectors without system size difference
Final Impact Vectors with system size difference
CCF Rate Calculations Using Probability Mode
Mapping Up / Down Equations

Note: ⊗ means multiplication.

Figure 5.2 - Approach For Quantifying CCF Parameters

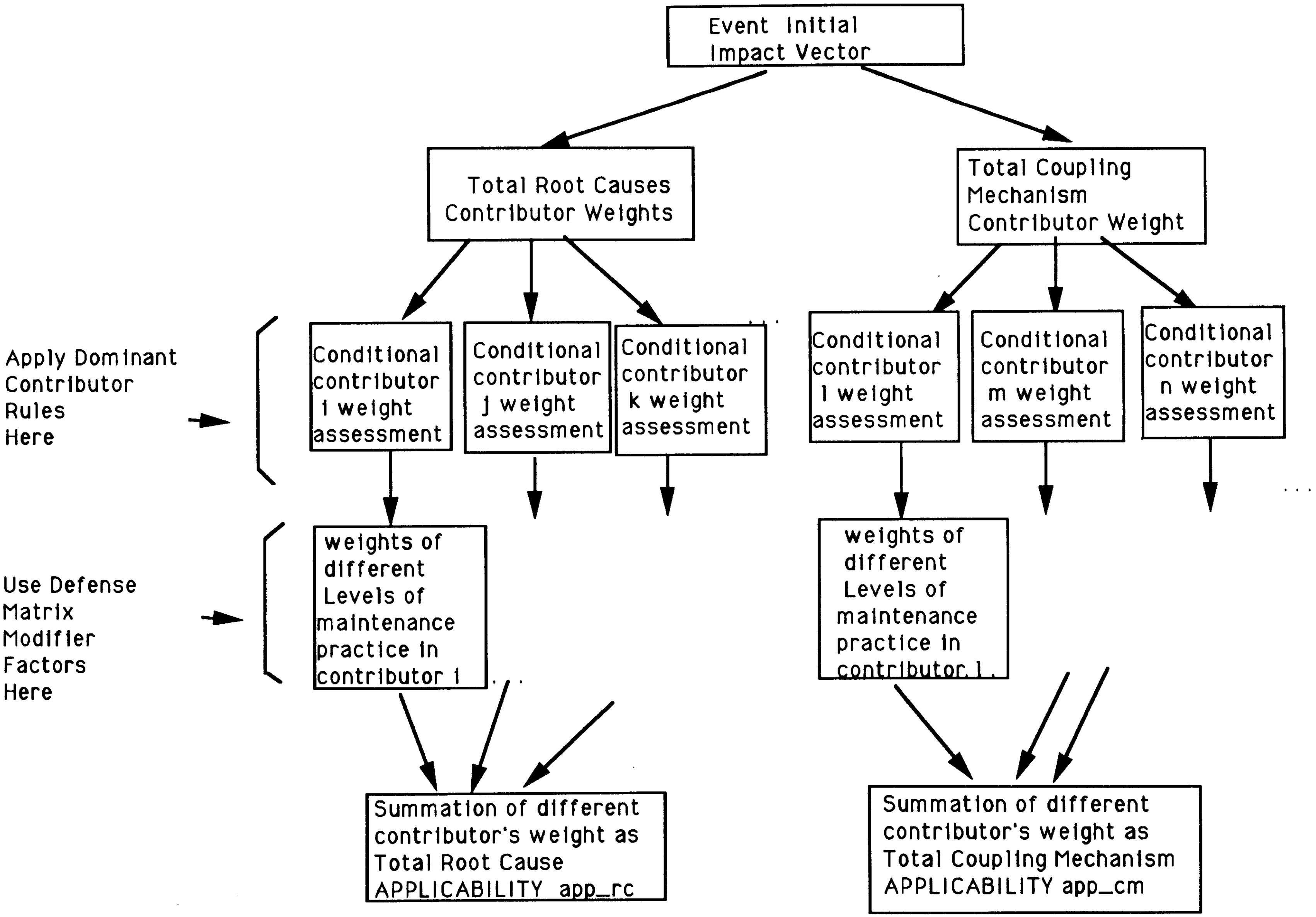

Event Initial Impact Vector
Total Root Causes Contributor Weights
Total Coupling Mechanism Contributor Weight
Apply Dominant Contributor Rules Here
Conditional contributor i weight assessment
Conditional contributor j weight assessment
Conditional contributor k weight assessment
Conditional contributor l weight assessment
Conditional contributor m weight assessment
Conditional contributor n weight assessment
Use Defense Matrix Modifier Factors Here
weights of different Levels of maintenance practice in contributor i
weights of different Levels of maintenance practice in contributor l
Summation of different contributor's weight as Total Root Cause APPLICABILITY app_rc
Summation of different contributor's weight as Total Coupling Mechanism APPLICABILITY app_cm

Figure 5.3 – Approach for Quantifying CCF Event " Applicability "

6. MAINTENANCE PROGRAM IMPACT ON HUMAN ERROR RATES

This section quantifies the impact of maintenance program changes on one PRA model parameter, the frequency that operators fail to correctly restore equipment after maintenance (ϕ_{re}), and the resulting impact on risk. This parameter is shown in Section 4 to be important to the JAF plant risk. It has also proven to be an important source of system unavailability in past PRA studies (e.g., WASH–1400 [43]). Moreover, as in the case of the common–cause failure analysis discussed in Section 5, an analysis of this parameter is interesting from a technical standpoint because it must deal with a key issue in PRA (the estimation of the likelihood of human error in this case).

6.1 Approach

The quantification of the risk impact associated with a change in ϕ_{re} is done in three steps, as shown in Figure 6.1. First, the particular maintenance program change underlying the change in ϕ_{re} must be specified. These program changes are stated in terms of changes in the factors that affect human performance (e.g., training, procedures). Next, the change in ϕ_{re} (and any associated factors) is calculated using an appropriate analytical model. Finally, the changes in ϕ_{re} are propagated through the system and plant models.

Regarding the first step, many aspects of the maintenance program (e.g., the quality of training, post–maintenance testing, and procedures) directly influence human reliability. Procedures that are ambiguous may result in different intepretations and uses by different groups. Faulty procedures can cause errors in maintenance by all who use the procedure. Of course, training can alleviate some of the confusion resulting from poor procedures. Post–maintenance testing serves as a check that the maintenance was performed correctly, although it may not catch slowly degrading conditions induced by human errors (note that these types of failures are not included in the quantification of ϕ_{re}). Quality control serves as a second check that the job is being performed properly. Quality control is performed by a separate group at JAF. Examples of explicit quality control at JAF include having a second person check a maintenance technician's work, and having a double sign–off on all important steps in a task. Another example, not implemented at JAF, involves having one person read the procedure while the other is performing the task to ensure verbatim compliance with procedures.

In order to perform the second step, a simple approach based on the well–known Technique for Human Error Rate Prediction (THERP) [10] is used. This approach allows the direct treatment of a number of issues addressed in the maintenance program block diagram (Figure 2.1). An alternate approach employing the MAPPS simulation code is also briefly discussed. The THERP–based approach is applied to the failure of operators to restore RHR pump path components following maintenance.

The third step is performed in a straightforward manner, using the simplified JAF plant model and the RHR system model described in Section 4 (these are based upon the preliminary models described in Ref. 6). It should be noted that there are two technical weaknesses in these models regarding their treatment of the "fail to restore" failure mode for RHR system components. First, these models do not treat the frequency of maintenance or the time required to detect an incorrect system configuration. Second, they do not treat the possibility that multiple RHR trains may be improperly restored. These points are further discussed in Section 6.4.

6.2 Quantification of ϕ_{re}

The basic THERP procedure for computing the frequency of human errors is discussed in Section 3. In the case of multiple errors, it is pointed out that the analyst needs to compute a base human error rate and a coupling factor. The latter factor is used to compute the conditional probability of subsequent human errors, given the occurrence of an initial error. This section presents two tools used to relate the base human error rate and the coupling factor to changes in the maintenance program: the human reliability tree and the dependence level tree.

6.2.1 Human Reliability Tree

The discussion in Section 6.1 indicates that there are five factors that affect the likelihood of human error during maintenance. These are:

- whether or not relevant procedures are available and used,
- the quality of the procedures,
- whether or not the maintenance technicians are trained on the specific task,
- whether or not a person from the QC department (or any other group) performs a second check on the maintenance work, and
- whether or not post–maintenance testing is done.

Figure 6.2 depicts the possible combinations of these factors and the human error rates associated with each combination. The human error rates are obtained using parameters from Tables 6.1–6.3 (adopted from Ref. 10).

The human error rates obtained through use of Figure 6.2, are determined by multiplying a basic human error probability by reduction factors that account for the implementation of different maintenance strategies. (Note that it is assumed that these parameters are independent and can therefore be multiplied to obtain the desired human error rate.) For example, Table 6.2 is used to quantify the human error rate when the operators use procedures that are above average quality. The value for this parameter is 0.002[12]. The reduction factors accounting for the other branches are quantified using Table 6.3. For example, Table 6.3 presents the human error rates for failing to detect errors made by others. For checking routine tasks using written materials, a human error rate of 0.1 is given. For checks that involves active participation, e.g., post–maintenance testing, an error rate of 0.01 is given. Table 6.4 presents the human error rates and factors used in estimating the human error rates underlying Figure 6.2.

It should be noted that Figure 6.2 is a human reliability decision tree developed specifically for treatment of maintenance tasks; it is not an event tree. Thus, the sum of the endstate error rates is not equal to one; in fact, the sum of these rates has no meaning. It should also be noted that the parameter values provided in Ref. 10 are based upon the experience of the authors of that report, and are widely used in PRA studies. These parameter values, however, do not reflect current data for RHR pumps nor do they necessarily reflect the specific circumstances at the JAF plant.

[12] This value is derived using entries from Table 6.2. This table gives a human error rate of 0.001 for an error of omission when using procedures that consist of short lists and check–off provisions. It is assumed that this is an optimal form for the procedure. It is further assumed that an error of commission is always possible and that the human error rate in this case is also 0.001. Therefore, the total error rate is 0.001 + 0.001 = 0.002.

Limited data are actually available concerning the failure of operators to properly restore RHR pumps after maintenance. However, a number of difficulties arise when these data are applied to the estimation of the parameters underlying Figure 6.2. Table 6.5 lists data on RHR pump failures obtained from Ref. 41. This reference provides LER–based data on failures of a variety of pump types; the data are collected over the period January 1, 1972 through September 30, 1980. Table 6.5 includes only those RHR pump failures involving human errors either by maintenance technicians or by operations personnel. Note that three of the events involve failure to return a valve or a switch to the correct positon. Four of the events involve procedure discrepancies and three are the result of using the wrong parts. The problem with these data from the standpoint of Figure 6.2 is that it is not known to which tree sequence each event applies. For example, in the case of Event 6, the quality of procedures in use (if any), the degree of training of the personnel on the restoration task, the involvement of QC, and whether or not post–maintenance testing was performed are not clear. This ambiguity prevents direct use of the event in a statistical analysis.

Improvements in Figure 6.2 can be made if JAF–specific data (or at least data from similar plants) are gathered. The data would preferably consist of actual success and failure counts; if such information is not available, the opinions of knowledgeable personnel (e.g., training instructors) could be used in a manner similar to the analyses done for seismic risk assessments and for severe accident probabilistic analyses.

6.2.2 Dependence Level Tree

Figure 6.2 provides the conditional frequency of human error, given the performance of maintenance on a single component. If one wants to look at multiple failures as a result of human errors during maintenance, those aspects of the maintenance program that couple maintenance tasks on redundant components must be examined. One potential coupling mechanism is provided by task scheduling. If similar tasks on redundant equipment are scheduled too closely together, the chances of multiple equipment failures due to identical mistakes being made during the nominally separate tasks are increased. One of the defenses against multiple failures therefore is to schedule maintenance on redundant equipment as far apart as possible. Procedure quality and use also will have a large impact on the likelihood that operators fail to restore multiple trains of equipment. As pointed out above, if the procedure is incorrect, mistakes are likely for all equipment affected. Training too, can have an effect. If all the maintenance groups are properly trained on the task and procedures, errors will be less likely.

To determine the conditional frequency of multiple failures due to human error during maintenance, the THERP model is used. Thus, as described in Section 3, a human reliability tree is drawn for the tasks in question. Here, each branch in the human reliability tree represents maintenance on a single component. To account for the coupling mechanisms described above, the dependence level parameters are modified to reflect the presence or absence of defenses against these coupling mechanisms.

Figure 6.3 presents a tree diagram similar in concept to Figure 6.2, except that Figure 6.3 is used to determine the degree of coupling (dependence) between maintenance failures. Figure 6.3 includes the following coupling mechanisms and defenses against multiple failures:

Coupling Mechanisms	Defenses
• Procedure quality	• Training
• Use of same staff for maintenance on redundant components	• Diversity of staff
• Performance of maintenance tasks on redundant equipment close in time	• Time separation of maintenance tasks on redundant equipment

The combination of coupling mechanisms and defenses applied are used to determine the level of dependence between maintenance tasks performed on redundant components. In the top branch of Figure 6.3, the procedure quality is good and different staff are used for maintenance on redundant equipment. Since there are no coupling mechanisms, zero dependence is assumed for tasks following this branch. Note that training is a defense against multiple failures caused by poor procedures. Since the procedure quality is good, the training question is not asked when following the upper branch. Furtheromore, if diverse staff are used for maintenance on redundant equipment, the question of tight scheduling is also not applicable.

If the same staff perform maintenance on redundant equipment, there can be dependence between tasks. Medium dependence is assumed if the procedure quality is good. This dependence level can be reduced (to low) if tasks are scheduled far apart in time.

If the quality of the procedures is low, training can be used to defend against multiple human errors. If this defense is employed, low dependence is assumed when diverse staff work on redundant equipment. For the remainder of the tree, the level of dependence increases as the likelihood of coupling mechanisms increases, but can be decreased by employing the defenses discussed above.

Using this figure, the appropriate equation for quantifying the effect of dependence [see Eqs. (3.14)] can be selected and used in the THERP human reliability tree.

As in the case of Figure 6.2, improved plant–specific estimates for the conditional frequency of multiple failures can be developed if data are available. However, since multiple failure events tend to be rare, it is likely to be much more difficult to develop improved data–based estimates.

6.2.3 Using MAPPS for Quantifying ϕ_{re}

As discussed in Section 3, the Maintenance Personnel Performance Simulation (MAPPS) is a computer–based simulation model designed to estimate the likelihood of errors during the maintenance process [31]. This model accepts inputs for a number of variables that can be affected by changes in a maintenance program, such as technician fatigue (which is affected by changes in planning, scheduling, staffing, etc.) and the quality of written procedures. The model directly handles other issues such as post–maintenance testing, since it simulates the performance of personnel performing these activities.

MAPPS appears to be a promising tool for analyzing ϕ_{re}, especially since a personal computer version of the code, called Micro–MAPPS has been recently released [44]. It was not used in this project due to the unavailability of Micro–MAPPS at the time this project was being performed.

6.3 Application to Restoration of RHR Pump Train Components

The above methodolodgy is applied to the Containment Spray (CS) mode of the Residual Heat Removal System. A simplified system drawing is shown in Figure 6.4 (adapted from Ref. 45). The CS system aids in reducing primary containment pressure and mixing containment air after transients or LOCAs have occurred. The CS mode of operation is manually initiated by the operator upon receiving a LPCI (Low Pressure Coolant Injection) initiation signal. The operator must check that the RHR pumps are running and starts the RHR Service Water (RHRSW) pumps for the train being used. The operator then puts the CS control switch in manual and the CS spray override switches in override. The operator then opens valve 10MOV–26A/B and throttles valve 10MOV–31A/B (depending on which train is being initiated) [45].

The failure mode of interest is the failure to restore the RHR pump path components. These include the motor–operated valve (MOV) 10MOV–13X, the pump RHR P–3X, and manual valves 10RHR–250X and 10RHR–28X, where X denotes the train (either A, B, C, or D). Non–restoration of any of these components would render the train inoperable. The non–restoration frequency for Train X ($\phi_{\mathrm{re,x}}$), which is conditioned on the performance of maintenance, is the sum of the conditional frequencies of non–restoration of each component:

$$\phi_{\mathrm{re,x}} = \phi_{\mathrm{re,10mov\text{-}13x}} + \phi_{\mathrm{re,p\text{-}3x}} + \phi_{\mathrm{re,10rhr\text{-}250x}} + \phi_{\mathrm{re,10rhr\text{-}28x}} \tag{6.1}$$

To determine each of the component non–restoration frequencies, the tasks and procedures involving these components must be analyzed.

For maintenance to be performed on an RHR pump, 10MOV–13X must be closed [46]. It is improbable that this valve could be left closed following maintenance without being immediately detected. Following maintenance, RHR Pump Flow Rate and Inservice Test ST–2A is performed. In this test, the RHR pump is lined up to recirculate water through the suppression pool. Each loop is tested for desired flow and pump discharge pressure [47]. If 10MOV–13X were left closed, the RHR pump would trip due to loss of suction. This would alarm in the control room. The position of this valve is also verified in monthly surveillance tests [48]. During this test, each RHR pump is run, one at a time, circulating water to the suppression pool through the minimum flow line. Again, the pump could not run if 10MOV–13X were not open. If however, this valve is left in the closed position, it will prevent CS operation because it does not receive an open signal upon receipt of a LPCI initiation signal.

Using Figure 6.2, the following assumptions are used to determine the frequency that valve 10MOV–13X is not restored properly following maintenance:

- the procedure used is of good quality,
- the operators are trained on this procedure,
- there is no second check that the valve is in the correct position, and
- a post–maintenance test is performed.

The third and fourth bullets come directly from the written procedure for pump maintenance [46]. These assumptions result in a non–restoration frequency of $2.0*10^{-5}$. Note that although it appears that the conduct of a post–maintenance test should virtually eliminate the likelihood of a restoration failure, the non–zero failure frequency models the possibility that the post–maintenance is not performed correctly, or is not performed at all.

Manual valves 10RHR–250X and 10RHR–28X are also closed when the RHR pump is to have maintenance performed on it. These valves discharge to the drain and minimum flow lines, respectively. If these valves are left closed, it would not be detected during the post–maintenance testing. The positioning of these valves are verified using a written checklist after the performance of maintenance. The non–restoration frequency for each of these valves is $2.0*10^{-4}$.

The last restoration error that could lead to the pump train being unavailable involves the pump itself. Using Figure 6.2 with the assumptions that the technicians use procedures and that there is post–maintenance testing, a non–restoration frequency of $4.0*10^{-4}$ is obtained.

The data of Table 6.1 suggests that poor procedures are significant contributors to the human–induced unavailability of RHR pumps. A study done by the Tennessee Valley Authority (TVA) [49] points out that procedure deficiencies caused a large percentage of the human errors during maintenance. TVA reviewed its maintenance procedures to identify ways to reduce human errors and made the following recommedations for improving maintenance procedures [49]:

1. Procedures should be easy to read, understand, and follow, i.e., they should be "user friendly."

2. Administrative controls and requirements should be separated from physical work details.

To make procedures easy to read and understand, short concise statements involving action steps should be used. Ref. 49 states that these action statements should begin with active verbs such as remove, reinstall, clean, and inspect. Complex detail is removed from the action step and is placed in tables or appears as listed items or action substeps.

The JAF RHR pump maintenance procedure does not use this format. The steps in the procedure are not action statements. For example, the following procedure step is taken from the JAF RHR pump maintenance procedure MP–10.1 [46]:

> "7.2.16 Measure the inside diameters of the case wear ring 1–2) and hydrostatic bearing wear ring (2–7) and the outside diameter of the impeller (3–1) to determine the clearances. The measurements are to be taken at four (4) locations, 45° apart at the edges and centers of the running surfaces as shown in Figure 10.3. The design clearances are shown in Table 10.2. Ovality is allowable within those clearances. Clearance limits in excess of the maximums shown are allowed by the manufacturer to 125% of design.
>
> Clearances above 125% to 150% of design require manufacturer consultation. Clearances above 150% of design are considered to be totally worn and parts shall not be reused.
>
> Marks, scratches, wear, etc. may be removed and the clearances measured to determine limit status."

The use of graphics could simplify this statement and help avoid errors. A picture illustrating the actual parts and the procedure by which the measurements are to be taken would eliminate unessecessary wording and eliminate sources of confusion. A table should accomodate the information concerning clearance limits. After measurements are taken they should be compared to the required measurements, e.g., the "125% to 150% of design," explicitly stated in the table. The course of action to be taken if the clearances are not within limits should also be explicity stated in such a table.

The JAF procedure does include a rough hand sketch of the manner in which measurements are to be taken and a table of clearances at the end of the procedure. It is suggested however that a picture of the actual parts be placed within the step instead of the worded description presently used. This could be easily accomplished with currently available software. The table of clearances in the JAF procedure is shown in Table 6.6. This information should be placed in the actual step and a place for the recording of measurements should be provided. As stated earlier, the information indicating what should be done if the measurements are not within specified limits should also be integrated in the table. The graphics and the table could take the place of most of the above paragraph and present the information in a more easily understandable fashion.

Making procedures more user friendly may result not only in less mistakes in their use but also more use. This will result in a lower frequency of human error.

Ref. 49 estimates that, 30% of the time, procedures are not used at all. According to Figure 6.2, the human error rate during maintenance when procedures are not used is estimated to be 0.002, given that post–maintenance testing is performed. If it is assumed that the operators do not use the procedure 30% of the time, the resulting pump non–restoration frequency for the RHR pump (i.e., for $\phi_{re,p\text{-}3x}$) is $9.0*10^{-4}$.

Using Eq. (6.1), the base case value for the non–restoration frequency for a single pump train is obtained:

$$\begin{aligned}\phi_{re,x} &= \phi_{re,10mov\text{-}13x} + \phi_{re,p\text{-}3x} + \phi_{re,10rhr\text{-}250x} + \phi_{re,10rhr\text{-}28x} \\ &= 2.0*10^{-5} + 9.0*10^{-4} + 2.0*10^{-4} + 2.0*10^{-4} \\ &= 1.3*10^{-3}\end{aligned} \tag{6.1}$$

To see how improving RHR pump procedures affects the non–restoration frequency, assume that improvements in procedures lead to their use 100% of the time. Figure 6.2 then predicts that the associated non–restoration frequency for the pump is $4.0*10^{-5}$, a reduction by a factor of 20 for $\phi_{re,p\text{-}3x}$. The resulting change in $\phi_{re,x}$ is given by

$$\phi_{re,x} = 4.7*10^{-4}$$

Table 6.1

Estimated HEPs related to failure of administrative control

Item	Task	HEP	EF
(1)	Carry out a plant policy or scheduled tasks such as periodic tests or maintenance performed weekly, monthly, or at longer intervals	.01	5
(2)	Initiate a scheduled shiftly checking or inspection function*	.001	3
	Use written operations procedures under		
(3)	normal operating conditions	.01	3
(4)	abnormal operating conditions	.005	10
(5)	Use a valve change or restoration list	.01	3
(6)	Use written test or calibration procedures	.05	5
(7)	Use written maintenance procedures	.3	5
(8)	Use a checklist properly**	.5	5

*Assumptions for the periodicity and type of control room scans are discussed in Chapter 11 in the section, "A General Display Scanning Model." Assumptions for the periodicity of the basic walk-around inspection are discussed in Chapter 19 in the section, "Basic Walk-Around Inspection."

**Read a single item, perform the task, check off the item on the list. For any item in which a display reading or other entry must be written, assume correct use of the checklist for that item.

Table 6.2

Estimated probabilities of errors of omission per item of instruction when use of written procedures is specified*

Item**	Omission of item:	HEP	EF
	When procedures with checkoff provisions are correctly used†:		
(1)	Short list, ≤10 items	.001	3
(2)	Long list, >10 items	.003	3
	When procedures without checkoff provisions are used, or when checkoff provisions are incorrectly used††:		
(3)	Short list, ≤10 items	.003	3
(4)	Long list, >10 items	.01	3
(5)	When written procedures are available and should be used but are not used††	.05‡	5

*The estimates for each item (or perceptual unit) presume zero dependence among the items (or units) and must be modified by using the dependence model when a nonzero level of dependence is assumed.

**The term "item" for this column is the usual designator for tabled entries and does not refer to an item of instruction in a procedure.

†Correct use of checkoff provisions is assumed for items in which written entries such as numerical values are required of the user.

††Table 16-1 lists the estimated probabilities of incorrect use of checkoff provisions and of nonuse of available written procedures.

‡If the task is judged to be "second nature," use the lower uncertainty bound for .05, i.e., use .01 (EF = 5).

Table 6.3

Estimated probabilities that a checker will fail to detect errors made by others*

Item	Checking Operation	HEP	EF
(1)	Checking routine tasks, checker using written materials (includes over-the-shoulder inspections, verifying position of locally operated valves, switches, circuit breakers, connectors, etc., and checking written lists, tags, or procedures for accuracy)	.1	5
(2)	Same as above, but without written materials	.2	5
(3)	Special short-term, one-of-a-kind checking with alerting factors	.05	5
(4)	Checking that involves active participation, such as special measurements	.01	5
	Given that the position of a locally operated valve is checked (item 1 above), noticing that it is not completely opened or closed:	.5	5
(5)	Position indicator** only	.1	5
(6)	Position indicator** and a rising stem	.5	5
(7)	Neither a position indicator** nor a rising stem	.9	5
(8)	Checking by reader/checker of the task performer in a two-man team, or checking by a second checker, routine task (no credit for more than 2 checkers)	.5	5
(9)	Checking the status of equipment if that status affects one's safety when performing his tasks	.001	5
(10)	An operator checks change or restoration tasks performed by a maintainer	Above HEPs ÷ 2	5

*This table applies to cases during normal operating conditions in which a person is directed to check the work performed by others either as the work is being performed or after its completion.

**A position indicator incorporates a scale that indicates the position of the valve relative to a fully opened or fully closed position. A rising stem qualifies as a position indicator if there is a scale associated with it.

Table 6.4 – Factors Affecting Human Error Rates

Factor Affecting Human Reliability in Maintenance	HEP[1]/Modification Factor
HEP (procedure not used)	0.10
HEP (procedure quality is good)	0.002
HEP (procedure needs improvement)	0.02
HEP multiplier (not trained on task)	2.0
HEP multiplier (second check required)	0.10
HEP multiplier (post–maintenance testing)	0.01

[1] HEP = Human Error Probability

Table 6.5 – RHR Pump Failures Involving Human Error (Page 1 of 2)

Plant/Date	Failure Cause	Failures Events	Failure Mode	Failure Description
1) Davis Besse 1 5/28/78	operations error	1	Power lost to decay heat pump	personnel accidentally tripped ps busses
2) Davis Besse 1 6/15/78	maintenance error	3	Power supply lost to pump	personnel error
3) Davis Besse 1 8/13/80	maintenance error	1	Pump stopped when suction valve was closed	maintenance failed to defeat interlock
4) Davis Besse 1 1/28/76	maintenance error	1	pump inoperable	incorrect substitute breaker installed
5) Calvert Cliffs 2 10/17/78	procedure discrepancy	2	pumps lost suction	air leaked from purification system to SDC
6) Palisades 1 10/9/75	operations error	1*	no flow, no pressure	two valves in wrong position
7) Browns Ferry 1 1/1/71	maintenance error	2	pumps tripped because isolation valves closed	faulty relays installed
8) Brunswick 1 6/18/77	operations error	1	pump tripped	accidental bumping of switch

Table 6.5 – RHR Pump Failures Involving Human Error (Page 2 of 2)

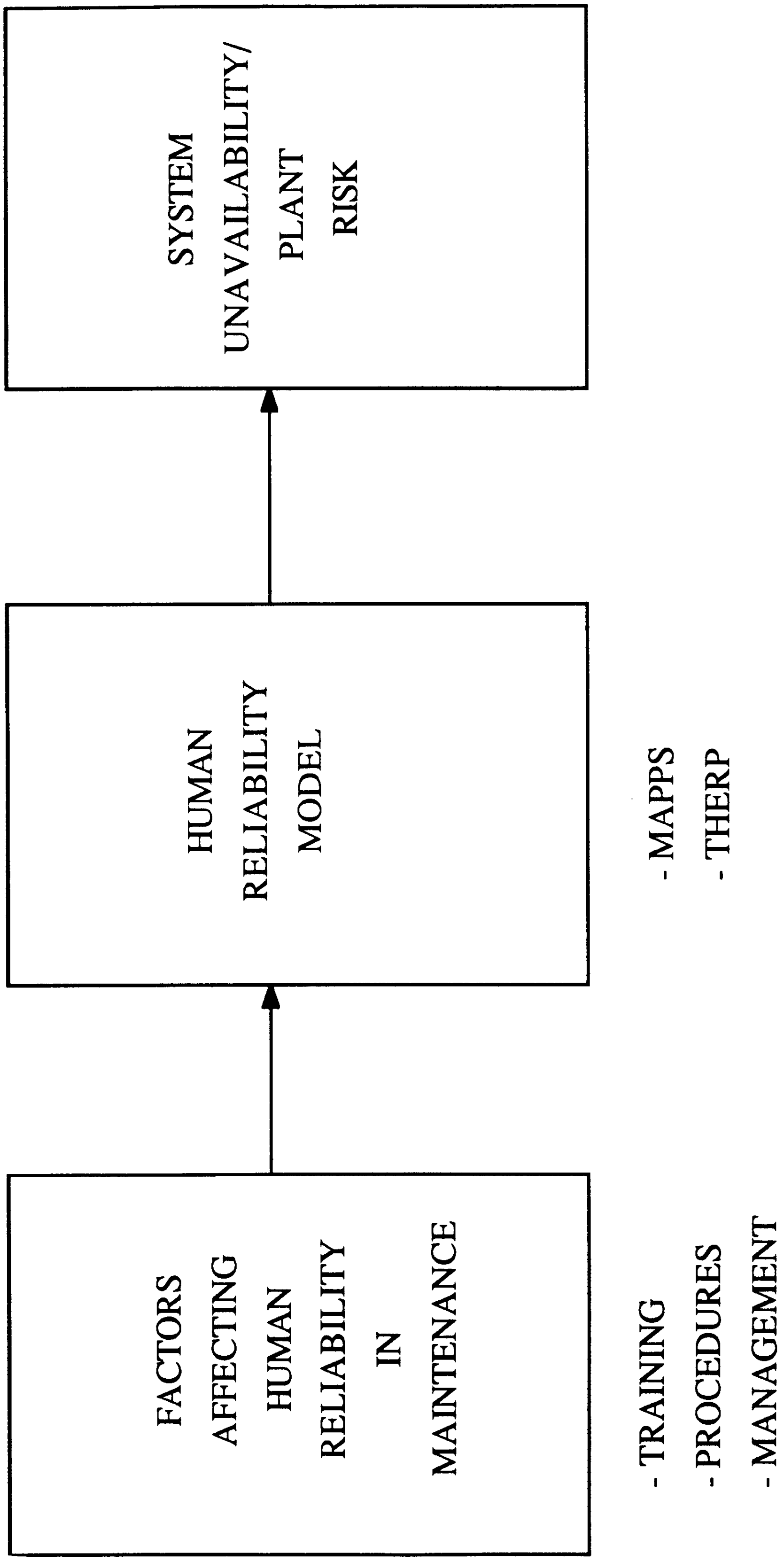
Plant/Date	Failure Cause	Failures Events	Failure Mode	Failure Des-cription
9) Brunswick 2 6/22/77	operations error	1	motor switch in off position	personnel left switch in off position
10) Edwin Hatch 1 4/9/76	maintenance error	1	pump tripped during functional test	pump wired incorrectl y
11) Edwin Hatch 1 9/6/80	maintenance error	1	pump vibrated outside ASME code	wrong reference data used
12) Nine Mile Point 1 9/15/78	maintenance error	1	pump inoperable	control power fuse was bent
13) Nine Mile Point 1 4/4/77	procedure discrepancy	1	low suction	
14) Peach Bottom 2 4/29/78	operations error	1	pump blocked for 2 hours	operator removed unit 2 instead of unit 3
15) Beaver Valley 1 4/8/80	procedure discrepancy	3	pumps airbound	pumps not vented
16) Donald Cook 2 9/4/80	procedure discrepancy	1	pump unstable	pumps not properly vented
17) Quad Cities 1 12/2/76	maintenance error	1	air locked suction header	RHRSW pump had air line connected to case

* recorded as only one event even though two valves are mispositioned.

Table 6.6 - RHR Pump Part Clearances [46]

Location		Running Clearances (Dia.)	
From	To	From	To
Impeller (3-1)	Case Wear Ring(1-2)	.033"	.037"
Impeller (3-1)	Hydrostatic Bearing Cover Wear Ring (2-7)	.020"	.024"
Pump Shaft (4-1)	Pump Cover (2-1)	.125"	.155"
Pump Shaft (4-1)	Seal Flange (5-1)	.125"	.138"

Figure 6.1 – Block Diagram for Quantifying Effect of Maintenance on Human Error Rates and Plant Risk


FACTORS AFFECTING HUMAN RELIABILITY IN MAINTENANCE
- TRAINING
- PROCEDURES
- MANAGEMENT
HUMAN RELIABILITY MODEL
- MAPPS
- THERP
SYSTEM UNAVAILABILITY/ PLANT RISK

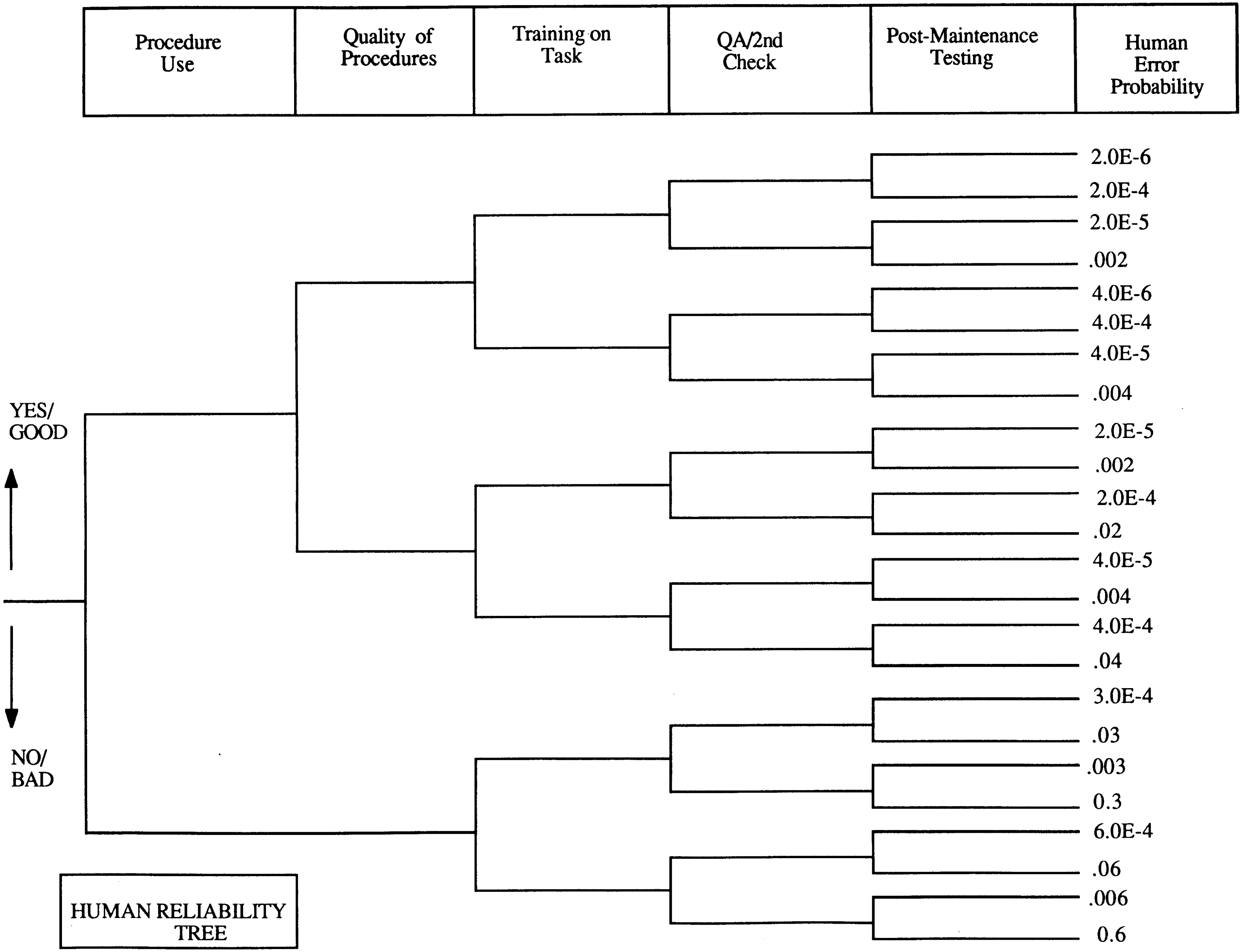
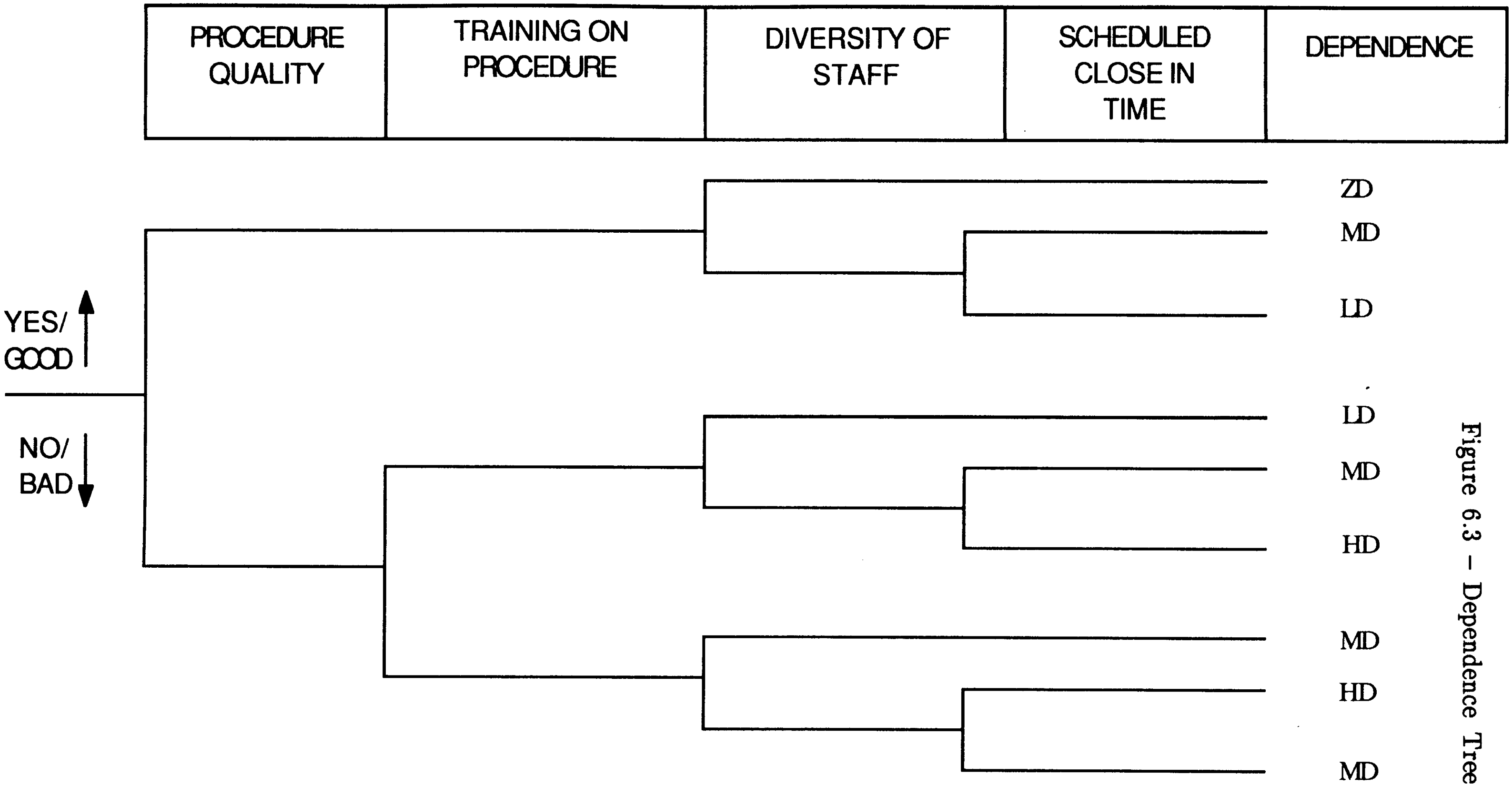
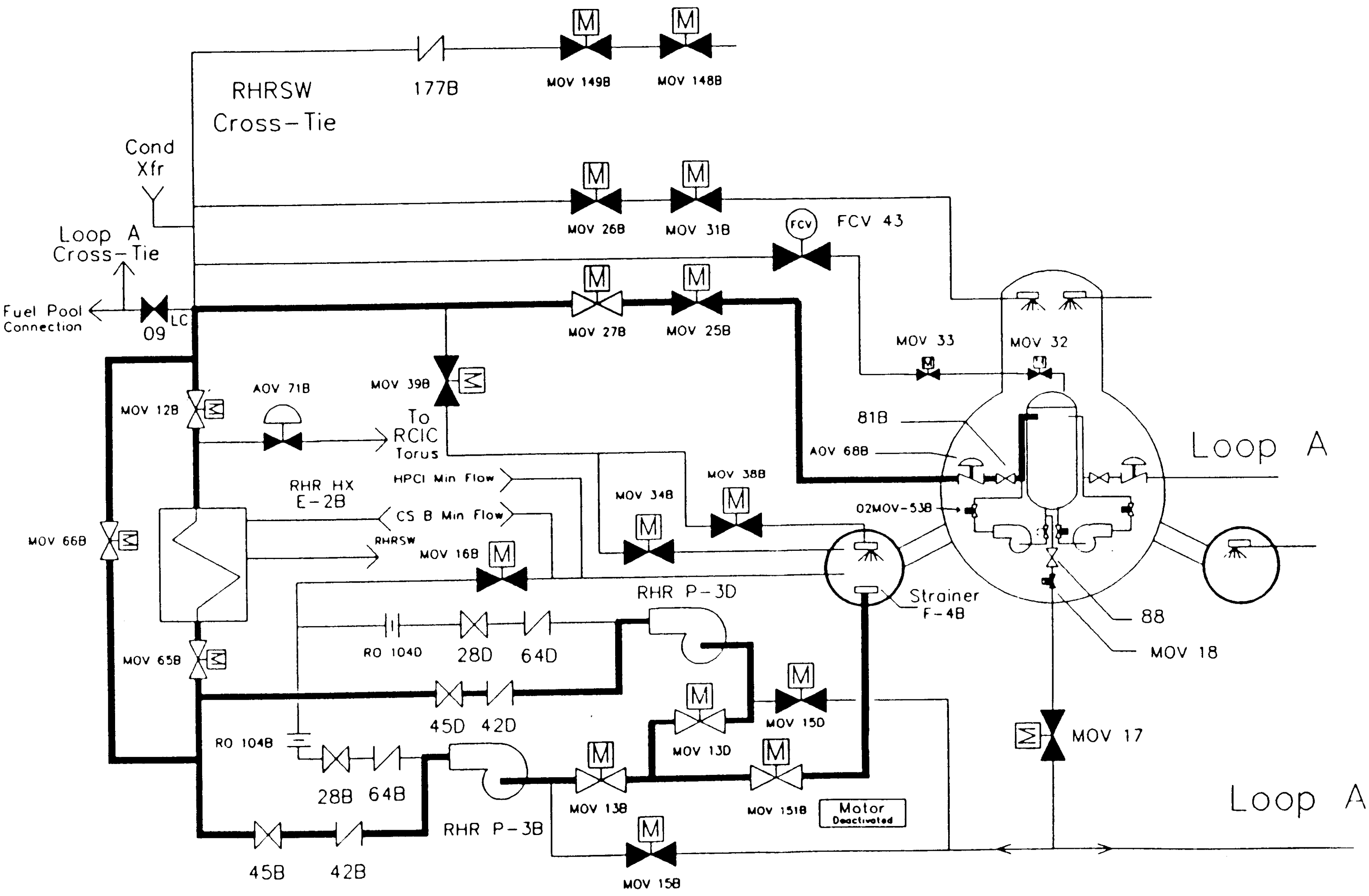


Figure 6.2 – Human Reliability Tree



DEPENDENCE LEVELS FOR TASKS
PERFORMED ON REDUNDANT EQUIPMENT

Figure 6.3 – Dependence Tree



Note: Valves are shown in their standby position.

Figure 6.4 – Simplified P&ID for RHR System

RESIDUAL HEAT REMOVAL SYSTEM,
LOW PRESSURE INJECTION SCHEMATIC

7. QUANTIFICATION OF MAINTENANCE IMPACT ON RISK

Section 5 develops a model for quantifying the impact of changes in maintenance practices on common–cause failure rates. Section 6 performs a similar role for human error rates (the failure to restore equipment following testing or maintenance). In this section, the impacts of a number of maintenance program changes (relative to the current JAF program) are quantified.

Two particular parameters are treated in this analysis. The first parameter, Q_{4mdp}, is the demand unavailability of the four RHR pumps due to common–cause failure. The second is Q_{re}, the unavailability of a single RHR pump train (one of four) due to the failure of the operators to restore the train after maintenance. Note that, in principle, multiple train unavailabilities due to restoration errors should be considered; however, these do not appear in the important cutsets reported in Ref. 6 (possibly because their joint probabilities are small), and are therefore not considered in this analysis.

The case studies discussed in this section are developed by examining the maintenance program block diagram (Figure 2.1), 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).

7.1 Maintenance Program Block Options

Five blocks in Figure 2.1 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 report. The blocks considered are:

- Block 1 – Maintenance Management
- Block 2 – Corrective, Preventive, and Predictive Maintenance
- Block 3 – Post–Maintenance Testing
- Block 8 – Personnel Qualification and Training
- Block 9 – Procedures and Regulatory Constraints

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

7.1.1 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. Poor planning and scheduling activities can also place the operators under significant time pressure, increasing their stress and the likelihood that the operators fail to restore a train of RHR after maintenance[13].

[13] Tight scheduling of maintenance activities could increase the dependency between nominally separate actions in restoring equipment. Thus, the THERP/ASEP model should be affected by changes in Block 1. As discussed earlier, the risk model used in this study does not include failures to restore multiple trains of equipment. The effect of tighter or looser scheduling on the coupling of failures is therefore not treated in this case study.

The options affecting Q_{4mdp} 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).

The options affecting Q_{re} are as follows:

A) Tight scheduling.
B) Loose scheduling.

The current practices at JAF are best represented by (A).

7.1.2 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 postitive.

Regarding the effect on Q_{re}, a stronger emphasis on preventive maintenance can increase the frequency with which an RHR train is taken out for servicing. This increases the rate of challenges to the operators to properly restore the train after servicing. On the other hand, since the servicing intervals are shorter, it also reduces the time that a failure will go undetected. Recall from Eq. (3.6) that the unavailability due to restoration errors following maintenance is given by

$$Q_{re} = f_m \phi_{re} \tau_{d,m} \tag{7.1}$$

Unless failures can be detected before the next maintenance period, the maintenance frequency f_m is likely to be inversely proportional to the detection time $\tau_{d,m}$, and the unavailability Q_{re} remains constant regardless of the particular mixture of corrective, preventive, or predictive maintenance employed. Thus, only options affecting the common–cause failure term, Q_{4mdp}, are treated for this block.

The options affecting Q_{4mdp} 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).

7.1.3 Block 3 – Post–Maintenance Testing

The performance of post–maintenance testing directly affects the likelihood of system restoration errors after maintenance, but does not affect the likelihood of other common–cause failures (as modeled by Q_{4mdp}).

The options affecting Q_{re} are as follows:

A) Post–maintenance testing not performed.
B) Post–maintenance testing performed.

The current practices at JAF vary, according to the component/system being serviced.

7.1.4 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 Q_{4mdp} and Q_{re} 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 varies, according to the component/system being serviced.

7.1.5 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 Q_{4mdp} and Q_{re} are as follows:

A) Procedures not used.
B) Procedures used, procedure quality needs improvement.
C) Procedures used, procedure quality good.

The option best representing the current practices at JAF varies, according to the component/system being serviced.

7.2 Effects of Maintenance Program Changes on Risk Model Parameters

Using the approach developed in Section 5, the common cause unavailability of 4 RHR pumps (fail to start mode), Q_{4mdp}, is computed for a variety of cases. The results are shown in Table 7.1.

The first case treated in Table 7.1 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 7.1 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). Note that for Block 1, the CCF options differ from the human error/failure to restore (RE) options. Only CCF options are available for Block 2, and only RE options are available for Block 3.

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 Q_{4mdp} can be significantly reduced by maintenance program changes; the best case leads to nearly a factor of 25 reduction. This reduction is 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 a small (a factor of 4) increase in Q_{4mdp}. 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 changes in Q_{4mdp} predicted for the intermediate cases are generally small, varying from the baseline prediction by a factor of 3 or less.

In a similar fashion, the approach developed in Section 6, is used to compute the unavailability associated with a failure to restore an RHR pump train after maintenance, Q_{re}, for a variety of cases. The results are shown in Table 7.2.

As in Table 7.1, Table 7.2 provides a short description of the maintenance program characteristics being treated in each case. Note that since the program practices can vary from component to component, three descriptions (and related options–based codes) are provided. For example, in the baseline case used to represent the current JAF program, it is assumed that the procedures for the valves are of good quality, but the procedure for the pumps needs improvement.

The best case in Table 7.2 shows a reduction in Q_{re} of over 2 orders of magnitude. This is primarily due to the greater use of procedures for the pump, the inclusion of second checks in the procedures, and specific training of the maintenance technicians on the pump procedures. Post–maintenance testing for the manual valves also contributes significantly. The worst case shows an increase of nearly 3 orders of magnitude. This case's lack of procedures, training, second checks, and post–maintenance testing leads to a prediction that one of the four components considered will probably not be properly restored. Intermediate cases 1 RE, 3 RE, and 4 RE, which all focus on improving RHR pump availability, lead to about the same degree of improvement (about a factor of 3); training specific to the RHR pumps is shown to have the greatest benefit by a slight margin.

7.3 Effects of Maintenance Program Changes on Risk

Maintenance program changes have the potential to affect many PRA parameters simultaneously. The quantification of risk requires the treatment of cases where all affected parameters are changed, as the total change in risk may be greater than the sum of the changes due to separate changes in the parameters.

Table 7.3 describes the cases considered; Table 7.4 presents the impact on RHR system unavailability (CS mode) and plant risk for each case. Also presented are the results of the preliminary JAF Individual Plant Examination [6]. These results differ slightly from the baseline case results of this study due to this study's treatment of JAF–specific factors that affect common cause failure and human errors, 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_{4mdp} and Q_{re} are significant contributors to risk, Table 7.4 shows that the changes in RHR system unavailability are, for the most part, relatively small. This is believed to be due to the fact that the risk of losing long term decay heat removal is dominated by scenarios initiated by a loss of offsite power. The RHR system failures having the maximum contribution in such a situation could very well be different from the failures that contribute the most under normal circumstances. This result illustrates a well–known lesson from PRAs: the dominant contributors to risk can vary tremendously, depending on the level of consequences being considered [50].

The changes in plant risk for the different cases also tend to be small. (This is not unexpected, given the results of the scoping calculations performed in Section 4.) In particular, the potential for risk improvement appears to be quite small. This situation arises because of another well–known characteristic of PRAs: although Q_{4mdp} and Q_{re} are significant contributors to risk, they are not the only contributors. As measures are taken to reduce these dominant risk contributors, other (previously less important) contributors become visible [50]. The results for the worst case indicate that, if maintenance activities affecting the RHR pumps are significantly degraded, there can be a significant increase in risk.

The detailed results in Table 7.4 clearly depend upon the modeling assumptions employed in Sections 5 and 6, and upon the assumptions made in assessing the baseline conditions at the JAF plant. It is interesting to note, however, that the results of two independent studies: a) a study on the effect of improved maintenance on the frequency of loss of feedwater initiating events [36], and b) a study on the impact of management factors on core damage frequency [51] indicate risk changes that are comparable in scale to those shown in Table 7.4. Thus, it appears that Table 7.4 provides a reasonable indication of the potential improvements/degradations in risk given improvements/degradations in maintenance program activities.

Table 7.1 – Common Cause Failure Cases (Page 1 of 2)

Case Name	Definition	Q_{4mdp}
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)	$1.6*10^{-4}$
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)	$6.2*10^{-6}$
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)	$6.1*10^{-4}$
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)	$5.4*10^{-5}$
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)	$8.4*10^{-5}$

Table 7.1 – Common Cause Failure Cases (Page 2 of 2)

Case Name	Definition	Q_{4mdp}
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)	$5.8*10^{-5}$
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)	$4.8*10^{-5}$

Table 7.2 – Failure to Restore Model Cases (Page 1 of 3)

Case Name		Definition	Q_{re}
Baseline RE	a)	Valves 10RHR–250X and 10RHR–28X. Good procedures used; training on specific procedures; procedure has 2nd check; loose scheduling. Code: (1B, 3A, 8B, 9B)	$4.0*10^{-4}$
	b)	Valve 10MOV–13X. Same assumptions as for (a), except that there is no 2nd check, and there is a flow test. Code: (1B, 3A, 8B, 9A)	$2.0*10^{-5}$
	c)	Pump RHR P3–X. Procedures usage: 70%; procedures need improvement; no training on specific procedures; post–maintenance testing. Code: (1B, 3B, 8A, 9A)	$9.0*10^{-4}$
		Total:	$1.3*10^{-3}$
Best RE	a)	Valves 10RHR–250X and 10RHR–28X. Good procedures are used; operators are trained on procedure; always a 2nd check; post–maintenance testing is performed. Code: (1B, 3B, 8B, 9B)	$2.0*10^{-6}$
	b)	Valve 10MOV–13X. Same as (a). Code: (1B, 3B, 8B, 9B)	$4.0*10^{-6}$
	c)	Pump P3–X. Same as (a). Code: (1B, 3B, 8B, 9B)	$2.0*10^{-6}$
		Total:	$8.0*10^{-6}$
Worst RE	a)	Valves 10RHR–250X and 10RHR–28X. Procedures not used; no recovery factors are applied; no training; tight scheduling. Code: (1A, 3A, 8A, 9A)	$2.0*10^{-1}$
	b)	Valve 10MOV–13X. Same as (a). Code: (1A, 3A, 8A, 9A)	$4.0*10^{-1}$
	c)	Pump P3–X. Same as (a). Code: (1A, 3A, 8A, 9A)	$8.0*10^{-1}$
		Total[a]:	$9.0*10^{-1}$

[a] Total value accounts for cross–product terms.

Table 7.2 – Failure to Restore Model Cases (Page 2 of 3)

Case Name		Definition	Q_{re}
Case 1 RE	a)	Valves 10RHR–250X and 10RHR–28X. Same as baseline. Code: (1B, 3A, 8B, 9B)	$4.0*10^{-4}$
	b)	Valve 10MOV–13X. Same as baseline. Code: (1B, 3A, 8B, 9A)	$2.0*10^{-5}$
	c)	Pump RHR P3–X. Procedures are used 100% of the time; good quality procedures; post–maintenance testing is performed. Code: (1B, 3B, 8A, 9B)	$4.0*10^{-5}$
		Total:	$4.6*10^{-4}$
Case 2 RE	a)	Valves 10RHR–250X and 10RHR–28X. Same as baseline. Code: (1B, 3A, 8B, 9B)	$4.0*10^{-4}$
	b)	Valve 10MOV–13X. Same as baseline. Code: (1B, 3A, 8B, 9A)	$2.0*10^{-5}$
	c)	Pump RHR P3–X. Procedures are used 70% of the time; procedures need improvement; maintainers are trained on procedures; post–maintenance testing. Code: (1B, 3B, 8B, 9A)	$4.4*10^{-4}$
		Total:	$8.6*10^{-4}$
Case 3 RE	a)	Valves 10RHR–250X and 10RHR–28X. Same as baseline. Code: (1B, 3A, 8B, 9B)	$4.0*10^{-4}$
	b)	Valve 10MOV–13X. Same as baseline. Code: (1B, 3A, 8B, 9A)	$2.0*10^{-5}$
	c)	Pump RHR P3–X. Procedures are used 70% of the time; procedures need improvement; maintainers are trained on pump; post–maintenance testing. Code: (1B, 3B, 8B, 9A)	$2.0*10^{-5}$
		Total:	$4.4*10^{-4}$

Table 7.2 – Failure to Restore Model Cases (Page 3 of 3)

Case Name	Definition	Q_{re}
Case 4 RE a)	Valves 10RHR–250X and 10RHR–28X. Good quality procedures are used; operators are trained on procedures; procedure has 2nd check. Code: (1B, 3A, 8B, 9B)	$4.0*10^{-4}$
b)	Valve 10MOV–13X. Same assumptions as for (a); there is a 2nd check, and a flow test. Code: (1B, 3A, 8B, 9B)	$2.0*10^{-6}$
c)	Pump RHR P3–X. Procedures are used 70% of the time; procedures need improvement; 2nd check; post–maintenance testing is performed. Code: (1B, 3B, 8A, 9A)	$6.3*10^{-5}$
	Total:	$4.6*10^{-4}$
Case 5 RE a)	Valves 10RHR–250X and 10RHR–28X. Good quality procedures are used; operators are trained on procedures; procedure has 2nd check; post–maintenance testing. Code: (1B, 3B, 8B, 9B)	$4.0*10^{-6}$
b)	Valve 10MOV–13X. Same assumptions as for (a); no 2nd check, but there is a flow test; post–maintenance testing is performed. Code: (1B, 3B, 8A, 9B)	$2.0*10^{-5}$
c)	Pump RHR P3–X. Procedures are used 70% of the time; procedures need improvement; 2nd check; post–maintenance testing is performed. Code: (1B, 3B, 8A, 9A)	$9.0*10^{-4}$
	Total:	$9.2*10^{-4}$
Case 6 RE a)	Valves 10RHR–250X and 10RHR–28X. Good quality procedures are used; operators are trained on procedures; procedure has 2nd check. Code: (1B, 3A, 8B, 9B)	$4.0*10^{-4}$
b)	Valve 10MOV–13X. Same assumptions as for (a); no 2nd check, but there is a flow test. Code: (1B, 3A, 8A, 9B)	$2.0*10^{-3}$
c)	Pump RHR P3–X. Procedures are used 70% of the time; procedures need improvement; 2nd check. Code: (1B, 3A, 8A, 9A)	$8.8*10^{-2}$
	Total:	$9.0*10^{-2}$

Table 7.3 – Definition of Combined Cases (Page 1 of 2)

Case Name	Definition	Q_{4mdp}	Q_{re}
Baseline Combined	Procedures used most of the time; pump procedure needs improvement; maintenance crew trained on RHR procedures; post–maintenance testing; staggered testing on two loops; emphasis on corrective maintenance. CCF Code:(1A, 2A, 8B, 9A) RE Code: (1B, 3B, 8B, 9A) (Pump) (1B, 3A, 8B, 9B) (Valves)	$1.6*10^{-4}$	$1.3*10^{-3}$
Best Combined	Procedures used all of the time; good quality pump procedure; maintenance crew trained on RHR procedures; post–maintenance testing; staggered testing on trains; emphasis on predictive maintenance. CCF Code:(1B, 2C, 8B, 9B) RE Code: (1B, 3B, 8B, 9B)	$6.2*10^{-6}$	$8.0*10^{-6}$
Worst Combined	Tight scheduling; procedures not used; procedures need improvement; maintenance crew not trained on RHR procedures; no post–maintenance testing; staggered testing on two loops; emphasis on corrective maintenance. CCF Code:(1A, 2A, 8A, 9A) RE Code: (1A, 3A, 8A, 9A)	$6.1*10^{-4}$	$9.0*10^{-1}$
Case 1 Combined	Procedures used most of the time; good quality procedures; maintenance crew trained on RHR procedures; post–maintenance testing; staggered testing on two loops; emphasis on corrective maintenance. CCF Code:(1A, 2A, 8B, 9A) RE Code: (1B, 3A, 8B, 9B)	$1.6*10^{-4}$	$4.6*10^{-4}$

Table 7.3 – Definition of Combined Cases (Page 2 of 2)

Case Name	Definition	Q_{4mdp}	Q_{re}
Case 2 Combined	Procedures used most of the time; pump procedure needs improvement; maintenance crew trained on RHR procedures; post–maintenance testing; staggered testing on two loops; emphasis on predictive maintenance. CCF Code:(1A, 2C, 8B, 9A) RE Code: (1B, 3B, 8B, 9A) (Pump) (1B, 3A, 8B, 9B) (Valves)	$5.8*10^{-5}$	$8.6*10^{-4}$
Case 3 Combined	Procedures used most of the time; pump procedure needs improvement; maintenance crew trained on RHR procedures; post–maintenance testing; staggered testing on two loops; emphasis on preventive maintenance. CCF Code:(1A, 2B, 8B, 9A) RE Code: (1B, 3B, 8B, 9A) (Pump) (1B, 3A, 8B, 9B) (Valves)	$8.4*10^{-5}$	$4.4*10^{-4}$
Case 4 Combined	Procedures used most of the time; pump procedure needs improvement; maintenance crew trained on RHR procedures; post–maintenance testing; staggered testing on all trains; emphasis on corrective maintenance. CCF Code:(1B, 2A, 8B, 9A) RE Code: (1B, 3B, 8A, 9A) (Pump) (1B, 3B, 8B, 9B) (Valves)	$5.4*10^{-5}$	$4.6*10^{-4}$
Case 5 Combined	Procedures used most of the time; pump procedure needs improvement; maintenance crew trained on RHR procedures; no post–maintenance testing; staggered testing on two loops; emphasis on corrective maintenance. CCF Code:(1A, 2A, 8B, 9A) RE Code: (1B, 3A, 8B, 9A) (Pump) (1B, 3A, 8B, 9B) (Valves)	$1.6*10^{-4}$	$9.0*10^{-2}$

Table 7.4 – Combined Cases Risk Results

Case	System Unavailability Q_{rhr}	Ratio to Baseline Q_{rhr}	Plant Risk F(TW)	Ratio to Baseline F(TW)
IPE Result	$5.5*10^{-3}$	0.98	$1.7*10^{-4}$	0.85
Baseline	$5.6*10^{-3}$	1.0	$2.0*10^{-4}$	1.0
Best Case	$5.4*10^{-3}$	0.96	$1*10^{-4}$	0.50
Worst Case	1	180	$1.2*10^{-2}$	60
Case 1	$5.6*10^{-3}$	1.0	$1.9*10^{-4}$	0.95
Case 2	$5.5*10^{-3}$	0.98	$1.4*10^{-4}$	0.70
Case 3	$5.5*10^{-3}$	0.98	$1.5*10^{-4}$	0.75
Case 4	$5.5*10^{-3}$	0.98	$1.3*10^{-4}$	0.65
Case 5	$5.7*10^{-3}$	0.98	$1.0*10^{-3}$	5.0

8. CONCLUDING REMARKS

8.1 Summary of Results

This study quantifies the change in one measure of plant risk, the frequency of loss of long term decay heat removal, due to changes in maintenance at the James A. Fitzpatrick (JAF) plant. Quantification is accomplished in two steps. First, the effects of maintenance are quantified in terms of changes in two key parameters: the frequency of common cause failure of residual heat removal (RHR) pumps, and the frequency with which operators fail to correctly restore the RHR system following maintenance. These parameters are selected as the result of an importance analysis performed using a preliminary version of the JAF Individual Plant Examination (IPE) [6]. Second, the changes in these two parameters are propagated through a simplified version of the plant model to obtain the associated change in plant risk.

Based on this study's assessment of the current maintenance program at JAF, the it appears that the potential for significant risk reduction due to improved maintenance is not extremely large; an optimal program might lead to an 50% reduction. The optimal program would place a stronger emphasis on predictive maintenance, and would employ improved procedures for RHR pump maintenance. There is potential for significant risk increase (around a factor of 60) if the maintenance program is significantly degraded (e.g., if post–maintenance testing is deemphasized).

This study shows how, at a simple level, maintenance program changes can be quantified without explicit modeling of the details of a plant's management and organizational structure (e.g., the work request process). However, such modeling may be required: a) to more strongly justify the quantitative factors used in the analysis, and b) to quantify the effect of other program changes not yet treated (e.g., the strengthening of program elements ensuring feedback of information to organization).

8.2 Issues and Limitations

The analysis results clearly depend upon underlying assumptions regarding the modeling scope and data employed. These assumptions place some limitations on the conclusions that can be drawn regarding the risk impact of maintenance program changes.

There are two potential issues regarding modeling scope. First, this study employs two parameters, the demand unavailability of RHR pumps due to common cause (Q_{4mdp}) and the unavailability of an RHR train due to restoration failures following maintenance (Q_{re}), to quantify the effect of maintenance program changes on plant risk. These parameters are significant contributors to plant risk, and the maintenance program changes considered are directed specifically at the RHR system. Nevertheless, by neglecting the risk impacts associated with other parameters, the overall change due to certain maintenance program changes can be underestimated.

Consider, for example, the dominant minimal cutsets shown in Table 4.3. These generally involve single failure events for each system. Thus, Q_{4mdp} and Q_{re} are not multiplied together when quantifying the sequence likelihood. In turn, this means that the model does not address any nonlinear impacts of maintenance, reducing the importance of a given program change. The approach used in this study clearly can be extended to treat other systems and even some initiating events (e.g., the loss of feedwater event is treated in Ref. 36), thereby dealing with the nonlinear impact of maintenance on plant risk. However, such a treatment was judged to be beyond the scope of this study.

Regarding data, Section 7.4 points out that that the quantitative results of this study clearly depend upon the submodels for common cause failure and human error developed in Sections 5 and 6, respectively. In particular, the common cause failure analysis relies upon root cause and coupling mechanism modification factors obtained from Ref. 42 (see Tables 5.9–5.12 and 5.14–5.17), and the human error analysis relies upon THERP modification factors obtained from Ref. 10 (see Tables 6.1–6.3). The quantitative estimates provided in these references are based upon the experience of the authors, but do not necessarily reflect the specific conditions at JAF. Additional data gathering and analysis are required to provide a stronger basis for these estimates. Additional data/estimates are also needed to address root causes/maintenance defense and coupling mechanism/maintenance defense combinations not included in this report (see Tables 5.8 and 5.13).

The analysis also employs a number of judgments (based on the results of interviews with plant personnel) concerning the JAF maintenance program. These judgments are used to select the appropriate failure/error rate modifiers from the above–mentioned tables. These judgments clearly need to be reviewed before making an evaluation of the JAF maintenance program, and of the need to change any elements in that program.

Note that Section 7.4 points out that the results of two independent studies related to the plant service and maintenance indicate risk changes that are comparable in scale to those shown in this study[1]. This provides additional confidence that, despite the modeling and data limitations, this report provides a reasonable indication of potential improvements/degradations in risk given improvements/degradations in maintenance program activities.

8.3 Applications

The analytical techniques developed in this study can be applied to assess the impact of maintenance changes on common cause failures and maintenance–related human errors. Thus, they can be used to help design a maintenance program optimized from the standpoint of safety and cost. For example, one of the questions asked by the model is if the operators are trained on the maintenance procedures specific to a given system (or part of a system). Assuming that such a level of training cannot be accomplished and maintained for all equipment in the plant, the model provides a method to prioritize training.

It is important to recognize that this study does attempt to quantify all possible modifications to a maintenance program. The models provided in this study should be used in concert with currently available models (e.g., those dealing with the actual scheduling of maintenance activities [1,15]) 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 thererfore requires a treatment of the trade–offs between these competing effects.

[1] The first study uses digraph modeling techniques and failure data collected from Japanese power plants in an analysis of the frequency of loss of main feedwater, and of the impact of improved service and maintenance on this frequency [36]. The second study uses plant–specific data and PRA models to scope the level of impact that management and organizational factors can have on risk [51].

8.4 Future Work

The models used in this study are relatively straightforward. Improved models, such as a simulation model for maintenance crew performance [31] or a physical model for a component [52] could improve decision making concerning program changes. However, it is believed that there are two fundamental areas where work needs to be done to assure that maintenance program changes can be quantified.

The first, and most obvious, area concerns data. As mentioned earlier, this study relies upon values for sensitivity parameters obtained from other studies. The quantitative basis for many of these parameters is not clear. Actual data concerning, for example, the change in human error rates when operators are trained on a specific piece of equipment, could be very useful in enhancing the credibility, as well as accuracy, of the results. Because failure events are relatively rare, some work must also be done on modeling the failure process. This will allow the use of partial failures/component degradations as supplements for the data base. The work reported in Ref. 29 provides major advances in this direction.

The second area concerns a number of maintenance program activities not treated in this work, e.g., Block 6 in Figure 2.1 (Communication). In order to model the impact that changes in these blocks will have on risk, the particular workings of the organization must be analyzed (e.g., to determine the causal chain linking a change in policy with a change in actual organizational learning and, eventually, a change in basic event failure rates). Work has been initiated on the problem of management and organizational influences on risk (e.g., [13,51]), but the results are not yet ready for quantitative application.

REFERENCES

1) P.K. Samanta, S.M. Wong, and J. Carbonaro, "Evaluation of Risks Associated with AOT and STI Requirements at the ANO-1 Nuclear Power Plant," NUREG/CR-5200, BNL-NUREG-52024, August 1988.

2) W.E. Vesely, R.E. Kurth, and S.M. Scalzo, "Evaluation of Core Melt Frequency Due to Component Aging and Maintenance," NUREG/CR-5510, June 1990.

3) A. Dykes, "Application of Time-Dependent Unavailability Analysis to Standby Safety Systems," Ph.D. dissertation, Massachusetts Institute of Technology, 1982.

4) V. Dimitrijevic, "A Methodology for Incorporating Aging in System Reliability Calculations," Ph.D. dissertation, Massachusetts Institute of Technology, September 1987.

5) H. Specter, "How to Reduce Nuclear O&M Costs Through the Use of PRA [With Application to Quality Assurance]," draft paper, New York Power Authority, October 1989.

6) New York Power Authority, "Preliminary JAF IPE Results," draft report, 1990.

7) New York Power Authority, "James A. Fitzpatrick Nuclear Power Plant Individual Plant Examination," August 1991.

8) B.J. Fussell, "How to Hand-Calculate System Reliability Characteristics," *IEEE Transactions on Reliability*, *R-24*, No. 3, 1973.

9) 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.

10) A. D. Swain and H. E. Guttmann, " Handbook on Human Reliability Analysis with Emphasis on Nuclear Power Plant Analysis," NUREG/CR-1278, SAND80-0200, August 1983.

11) U.S. Nuclear Regulatory Commission, "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," 10 CFR Part 50, RIN: 3150 - AD00, 1991.

12) M. Dey, "Maintenance Approaches and Practices in Selected Foreign Nuclear Power Programs and Other U.S. Industries: Review and Lessons Learned," NUREG-1333, April 1990.

13) G. Apostolakis, O. Grusky, and D. Okrent, "Inclusion of Organizational and Managerial Factors into Probabilistic Safety Assessments of Nuclear Power Plants," NUREG/CR-5751, draft report, 1991.

14) D.P. Wagner, et al., "Risk-Based Analysis Methods Applied to Nuclear Power Plant Technical Specifications," *Nuclear Technology*, *84*, 233-238(1989).

15) 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.

16) J.H. Bickel, "Use of Probabilistic Safety Analysis in Obtaining A One–Time Variance in the Technical Specification Action Statements," Northeast Utilities Service Company, 198?

17) E.D. Sylvester (Project Manager, BWR Project Directorate #2, Division of BWR Licensing, USNRC), letter to E.E. Utley (Senior Executive Vice President, Power Supply and Engineering and Construction, Carolina Power and Light Company), March 27, 1987.

18) G.E. Vaughn (Vice President, Nuclear Operations, Houston Lighting and Power), letter to USNRC, ST–HL–AE–3283, February 1, 1990.

19) H. Rood (Senior Project Manager, Project Directorate V, Division of Reactor Projects – III, IV, V, and Special Projects, Office of Nuclear Reactor Regulation, USNRC), letter to J.D. Shiffer (Vice President, Nuclear Power Generation, Pacific Gas and Electric Company), October 4, 1989.

20) T.P. Speis (Director, Division of Safety Review and Oversight, USNRC), memo to H.L. Thompson, Jr. (Director, Division of PWR Licensing–A, NRR), January 15, 1985.

21) W. Greek, "Application of Reliability Centered Maintenance to San Onofre Unites 2 and 3 Auxiliary Feedwater Systems," EPRI NP–5430,

22) R.E. Barlow and F. Proschan, *Statistical Theory of Reliability and Life Testing: Probability Models*, To Begin With, Silver Spring, MD, 1981.

23) A. Pages and M. Gondran, *System Reliability: Evaluation and Prediction in Engineering*, North Oxford Academic, London, 1986.

24) E.V. Lofgren, "Probabilistic Risk Assessment Course Documentation, Volume 3: System Reliability and Analysis Techniques," NUREG/CR–4350, August 1985.

25) G. Apostolakis, "Mathematical Methods of Probabilistic Safety Analysis," UCLA–ENG–7464, September 1974.

26) A.E. Green and A.J. Bourne, *Reliability Technology*, Wiley, 1972.

27) J.K. Vaurio, "Unavailability of Components with Inspection and Repair," *Nuclear Engineering and Design*, *54*, 309(1979).

28) W.E. Vesely, "Risk Evaluation of Aging Phenomena: The Linear Aging Reliability Model and Its Extension," NUREG/CR–4769, EGG–2476, April 1987.

29) P.K. Samanta, et al., "Degradation Modeling with Application to Aging and Maintenance Effectiveness Evaluations," NUREG/CR–5612, BNL–NUREG–52252, March 1991.

30) A.D. Swain, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR–4772, February 1987.

31) A.I. Siegel, et al, "Maintenance Personnel Performance Simulation (MAPPS) Model: Summary Description," NUREG/CR–3626, ORNL/TM–904, May 1984.

32) New York Power Authority, "James A. Fitzpatrick Nuclear Power Plant Level 1 Probabilistic Risk Assessment Study Methodology and Guidelines Document," draft report, June 1, 1990.

33) W.J. Puglia, "A Reliability Program for Nuclear Power Plant Safety Systems," Massachusetts Institute of Technology, S.M. thesis, February 1990.

34) E.J. Henley and H. Kumamoto, *Reliability Engineering and Risk Assessment*, Prentice–Hall, 1981.

35) S. Cooper, N. Rasmussen, and N. Siu, "Uncertainty and Importance Analyses of the Reliabilities of Systems Experiencing Aging," MITNE–279, Massachusetts Institute of Technology, December 1987.

36) N. Siu, J. Yoshimura, M. Ouyang, K. Credit, and N. Rasmussen, "PRA Applications in Nuclear Power Plant Service and Maintenance," Transactions of the First JSME–ASME Joint International Conference on Nuclear Engineering, Tokyo, Japan, November 4–7, 1991, Volume 2, pp. 491–497.

37) A. Mosleh, et al., "Procedures for Treating Common Cause Failures in Safety and Reliability Studies," NUREG/CR–4780, November 1987.

38) 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.

39) N. Siu and A. Mosleh, "Treating Data Uncertainties in Common Cause Failure Analysis," *Nuclear Technology, 84*, No. 3, 265–281, March 1989.

40) K.N. Fleming and A. Mosleh, "Classification and Analysis of Reactor Operating Experience Involving Dependent Events," EPRI NP–3967, June 1985.

41) 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, EEGG–EA–5524, September 1981.

42) 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.

43) U.S. Nuclear Regulatory Commission, "Reactor Safety Study," WASH–1400 (NUREG–75/014), 1975.

44) D.I. Gertman, "Conversion of a Mainframe Simulation for Maintenance Performance to a PC Environment," Proceedings of the Eighteenth Water Reactor Safety Meeting, Rockville, MD, October 22–24, 1990, pp. 199–204.

45) New York Power Authority, "JAFNPP Individual Plant Examination, Residual Heat Removal Low Pressure Coolant Injection Mode system model description." 1990.

46) New York Power Authority, "James A. Fitzpatrick Nuclear Power Plant Maintenance Procedure: Maintenance of RHR PUMP MP–10.1," March 2, 1990.

47) New York Power Authority, "James A. Fitzpatrick Nuclear Power Plant Operations Surveillance Test Procedure: RHR Pump Flow Rate and Inservice Test (IST) ST–2A," July 18, 1991.

48) New York Power Authority, "James A. Fitzpatrick Nuclear Power Plant Operations Surveillance Test Procedure: RHR Pump and MOV Operability and Keep Full Level Switch Functional Test ST–2B," April 17, 1991.

49) C.E. Chmielewski and R.C. McKay, "Maintenance Instruction Innovations," Proceedings of the American Power Conference, Vol. 52, 1990.

50) B.J. Garrick and J.C. Lin, "Lessons Learned and Future Developments in Probabilistic Safety Assessment," presented at the PWR Safety Seminar, Prague, Czechoslovakia, April 18–19, 1991.

51) W. He and N. Rasmussen, "Estimating Management Impact on Core Damage Frequency," submitted for publication, Transactions of the American Nuclear Society 1992 Summer Meeting, June 7–12, Boston, MA, 1992.

52) Y. Uhara, et al., "A New Approach for Predicting Reliability of Mechanical Components," Transactions of the American Nuclear Society 1990 Winter Meeting, November 11–15, 1990, Washington, D.C., pp. 376–378.

APPENDIX A

Table A.1 - RSW System Component Ranking

COMPONENT & FAILURE MODES	DATA	RANKING
2 Discharge valves ⟶ CC	3.8E-5	1
4 Pumps ⟶ FS	7.6E-6	2
Mov 89A Control Circuit ⟶ NO 89B Control Circuit ⟶ NO	4.4E-6	3
MOV 89A ⟶ CC 89B ⟶ CC	7.4E-7	4
Switchgear 10A-S48A ⟶ DN 10A-S48B ⟶ DN	5.5E-7	5
Manual valve 24B ⟶ PG valve 11B ⟶ PG Pump P-1A ⟶ FR Pump P-1C ⟶ MA	1.6E-7	6

Table A.2 - ESW System Component Ranking

COMPONENT & FAILURE MODES	DATA	RANKING
Loop B ⟶ MA	2.8E-6	1
MDP 46-2A ⟶ FR 46-2B ⟶ FR	2.2E-6	2
Loop A ⟶ MA	1.9E-6	3
Manual valve 3A ⟶ RE valve 3B ⟶ RE	5.7E-7	4

Table A.3 - AC4 System Component Ranking

COMPONENT & FAILURE MODES	DATA	RANKING
Circuit Breaker 10640 ⟶ DN 10550 ⟶ DN	1.5E-6	1
Relay 86A-1HOEB01 path ⟶ NO 86A-1HOEB03 path ⟶ NO	8.8E-7	2
Relay Bus10600 ⟶ MC Bus10500 ⟶ MC	5.7E-7	3
Relay 86A-1HOEA01 path ⟶ NO	1.9E-8	4

Table A.4 - DC1 System Component Ranking

COMPONENT & FAILURE MODES	DATA	RANKING
Panel 10500 ⟶ ST 10600 ⟶ ST 71DC-A4 ⟶ ST BCB-2A ⟶ ST	1.3E-7	1
Panel BCB-2B ⟶ ST	1.7E-8	2
DC fuse ⟶ NO	9.8E-8	3

Table A.5 - HPCI System Component Ranking

COMPONENT & FAILURE MODES	DATA	RANKING
System ⟶ MA	2.9E-7	1
Turbine Driven Pump ⟶ FS	4.8E-8	2
Turbine Driven Pump ⟶ FR	4.2E-8	3
Steam Supply/exhaust path ⟶ DN	1.7E-8	4

Table A.6 - TBC System Component Ranking

COMPONENT & FAILURE MODES	DATA	RANKING
Control Circuit for Pump 37P-2A → NO 37P-2B → NO	1.0E-9	1
Pump 37P-2B → MA	8.8E-10	2
Pump 37P-2B → RE	2.1E-10	3

For other systems, each only has one ranking inside itself.

Table A.7 - Pumps Group Component Ranking

COMPONENT & FAILURE MODES	DATA	RANKING
LPCI 4 Pumps → FS	2.8E-5	1
LPCI Pump 3A → RE	2.2E-5	2
LPCI Pump 3D → RE	2.1E-5	3
RSW 4 Pumps → FS	7.6E-6	4
ESW Pump 2A → FR Pump 2B → FR	2.2E-6	5
RSW Pump 1A → FR Pump 1C → MA	1.6E-7	6
HPCI TDP → FS	4.8E-8	7
HPCI TDP → FR	4.2E-8	8
TBC Pump 37P-2B → MA	8.8E-10	9
TBC Pump 37P-2B → RE	2.1E-10	10

Table A.8 - Valves Group Component Ranking

COMPONENT & FAILURE MODES	DATA	RANKING
RSW 2 Discharge Valves → CC	3.8E-5	
LPCI Check Valve 42B → CO 42C → CO	2.9E-6	2
LPCI Check Valve 42A → CC 42D → CC	1.1E-6	3
RSW MOV 89A --> CC 89B → CC	7.4E-7	4
ESW Manual Valve 3A --> RE 3B → RE	5.7E-7	5
LPCI MOV 12B --> PG MOV 65B → PG MOV 3A → PG MOV 65A → PG MOV 12A → PG	2.0E-7	6
RSW Manual Valve 24B --> PG Manual Valve 11B → PG		
LPCI Check Valve 45D → PG Manual Valve 151A → PG	1.6E-7	7
LPCI MOV 16A → CC MOV 16B → CC	1.3E-8	8

Table A.9 - CONTROL CIRCUITS GROUP COMPONENT RANKING

COMPONENT & FAILURE MODES	DATA	RANKING
RSW MOV 89A Control Circuit → NO		
89B Control Circuit → NO	4.4E-6	1
LPCI RP-3A Control Circuit → NO	2.3E-6	2
AC4 Circuit Breaker 10640 → DN		
10550 → DN	1.5E-6	3
LPCI RP-3D Control Circuit → NO	2.3E-7	4
TBC P37-2A Control Circuit --> NO		
P37-2B Control Circuit → NO	1.0E-9	5

Table A.10 - Trains Group Component Ranking

COMPONENT & FAILURE MODES	DATA	RANKING
ESW Loop B → MA	2.8E-6	1
ESW Loop B → MA	1.9E-6	2
HPCI Whole system → MA	2.9E-7	3
HPCI Steam Supply Path → DN	1.7E-8	4

Table A.11 - Relay Group Component Ranking

COMPONENT & FAILURE MODES	DATA	RANKING
AC4 86A-1H0EB01 → NO 86A-1H0EB03 → NO	8.8E-7	1
LPCI 10A-K19A Path → CO	6.9E-7	2
LPCI 10A-K22B Path → OC	5.9E-7	3
AC4 Bus 10500 → MC 10600 → MC	5.7E-7	4
AC4 86A-1H0EA01 → NO	1.9E-8	5
LPCI 10A-K48A Path → NO	4.5E-9	6
LPCI 10A-K48B Path → NO	4.2E-9	7

Table A.12 - Switchgears Group Component Ranking

COMPONENT & FAILURE MODES	DATA	RANKING
RSW 10A-S48B Path → DN 10A-S48A Path → DN		
SPC 10A-S17A Path → DN	5.5E-7	1
LPCI 10-S3D Path → DN	1.2E-10	2

Table A.13 - Buses Group Ranking

COMPONENT & FAILURE MODES	DATA	RANKING
DC1 BCB-2A → ST 10500 Panel → ST 10600 Panel → ST 71DC-A4 Divsion → ST	1.3E-7	1
DC1 BCB-3B → ST	1.7E-8	2

Remaining components each have a single ranking.