NUREG/CR--5695

TI91 010631

A Process for Risk-Focused Maintenance

Manuscript Completed: February 1991
Date Published: March 1991

Prepared by
E. V. Lofgren, S. E. Cooper, R. E. Kurth, L. B. Phillips

Science Applications International Corporation
1710 Goodridge Drive
McLean, VA 22102

Prepared for
Division of Regulatory Applications
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555
NRC FIN L1321

DISCLAIMER

ABSTRACT

This report presents a process for focusing maintenance resources on components that enable nuclear plant systems to perform their essential functions and on components whose failure may initiate challenges to safety systems, so as to have the greatest impact in decreasing risk. The process provides criteria, based on risk, for deciding which components are critical to risk and determining what maintenance activities are required to ensure reliable operation of those "risk-critical" components.

Two approaches are provided for selection of risk-critical components. One approach uses the results of a Probabilistic Risk Assessment (PRA); the other is based on the methodology developed for this report, which has a basis in PRA although it does not use the results of a PRA study. Following identification of risk-critical components, both approaches use a single methodology for determining what maintenance activities are required to ensure reliable operation of the identified components.

The report also provides demonstrations of application of the two approaches to selection of risk-critical components and demonstrations of application of the methodology for determining what maintenance activities are required to an active standby safety system, a normally operating system, and passive components.

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

LIST OF FIGURES

LIST OF TABLES

LIST OF TABLES (CONTINUED)

EXECUTIVE SUMMARY

The report describes a "risk-focused" process for establishing a "reliability-focused" maintenance program. The objective of the risk-focused maintenance process is to focus maintenance resources on components that enable nuclear plant systems to fulfill their essential functions and on components whose failure may initiate challenges to safety systems, so as to have the greatest beneficial impact in reducing risk.

The risk-focused maintenance process is applicable to all categories of equipment that control off-site radioactive doses, or that could adversely impact the ability of the plant to prevent or mitigate accidents or transients. The process addresses only a portion of the total plant maintenance program (i.e., use of the risk-focused process should not preclude other maintenance activities the utility considers necessary for proper maintenance of its equipment).

The risk-focused maintenance process consists of two major steps: 1) identifying risk-critical components and 2) determining what maintenance activities are required to ensure reliable operation of the risk-critical components identified.

Two approaches are provided for identifying risk-critical components. Both are based in Probabilistic Risk Analysis (PRA), although only one of them uses the results of a PRA study. Hence, this step should be performed by, or with the assistance of, personnel familiar with PRA techniques and concepts.

> The first approach begins with consideration of functions that must be performed for safe operation of the nuclear plant and identification of components performing those functions. The approach identifies 1) structures, systems, and components that are relied upon to prevent or mitigate accidents and 2) components whose failure would result in an accident or transient which challenges front-line safety systems. These components are screened using logic described in this report to determine which are risk-critical components. Then, components required to support those risk-critical components, balance of plant components whose failure would result in an accident or transient, and passive equipment whose failure would violate Final Safety Analysis Report success criteria are added to the list. That completes this step under this approach.
>
> The second approach uses results of a PRA study, which considers function inherently, to identify the risk-critical components. First, a top fraction of the core melt frequency, representing the most likely accident scenarios, is chosen. Selection of this fraction is based upon the fraction reported in existing PRAs or recommended for the Individual Plant Examination submittal, considering as appropriate any natural breaks in the rankings of cutsets. An alternative to choosing a top fraction of the core melt frequency is to use importance measures or sensitivity analysis to accomplish this.

The report provides demonstrations of successful application of both approaches. The first (Non-PRA study) was demonstrated with data from an operating PWR plant; the second (PRA study) with data and a completed PRA study from an operating BWR plant.

After identification of risk-critical components by one of the above approaches, a single methodology is used to establish a reliability-focused maintenance program. This methodology is akin to Reliability-Centered Maintenance. The first step is to determine the dominant component failure modes that should be defended against. The second step is to determine maintenance activities that will defend against those dominant failure modes.

The report provides three demonstrations of application of the reliability-focused maintenance methodology: 1) to a standby safety system, 2) to a normally operating system, and 3) to passive components. The demonstrations show that the methodology is sound and can be applied to develop a satisfactory reliability-focused maintenance program.

SECTION 1

INTRODUCTION

In August of 1989, the U.S. Nuclear Regulatory Commission (NRC) issued a draft Regulatory Guide, DG-1001, entitled "Maintenance Programs for Nuclear Power Plants" (Reference 1-1). This Regulatory Guide was developed to provide nuclear reactor licensees with guidance on methods acceptable to the NRC staff for planning, conducting, and assessing the effectiveness of nuclear power plant maintenance programs to prevent the degradation or failure of structures, systems and components that can significantly affect safety.

In April of 1990, Science Applications International Corporation (SAIC) was awarded a contract by the NRC to develop and demonstrate risk-focused methods for implementing maintenance programs at nuclear power plants.

This is a final report that provides detail beyond that contained in the draft regulatory guide concerning approaches for identifying risk-important systems and components and for implementing maintenance programs for these components which explicitly account for the unique reliability characteristics of each component/environment combination. This report summarizes these approaches and presents demonstrations of each approach. These demonstrations are meant to indicate the appropriate level of detail for applying the methods.

Section 2 describes the objective and scope of the risk-focused maintenance process presented in this report and provides brief descriptions of approaches and methodology for using the process. Section 3 describes an approach for identifying risk-critical components when a probabilistic risk assessment (PRA) is not used as a basis for choosing such components and summarizes a demonstration of that approach, described in more detail in Appendix A. Section 4 describes an approach for identifying risk-critical components when a PRA is used and summarizes the demonstration of that approach, described in more detail in Appendix B. Section 5 describes an approach for developing a reliability-focused maintenance program for risk-critical components and summarizes demonstrations of that approach for an active standby safety system, a normally operating system, and passive components. More detailed descriptions of those demonstrations are given in Appendices C, D, and E, respectively. Section 6 provides a glossary of certain terms used in this report, defined in the context of their use in this report.

REFERENCE

1-1. Draft Regulatory Guide, U.S. Nuclear Regulatory Commission, DG-1001, "Maintenance Programs For Nuclear Power Plants", August 1989.

SECTION 2

OVERVIEW OF RISK-FOCUSED MAINTENANCE PROCESS

This section discusses the objective and scope of the risk-focused maintenance process presented in this report and provides brief descriptions of approaches and methodology for using the process.

2.1 OBJECTIVE

The objective of the risk-focused maintenance process described in this report is to focus maintenance resources on components that enable nuclear plant systems to fulfill their essential safety functions and on components whose failure may initiate challenges to safety systems, so as to have the greatest beneficial impact in decreasing risk. (See Section 6, "Glossary Of Terms", for definition of "risk" as it is used in this report).

2.2 SCOPE

The risk-focused maintenance concept should be applied to all categories of equipment that control off-site radioactive doses, or that could adversely impact the ability of the plant to prevent or mitigate accidents or transients. This includes any components whose failure could result in initiating an accident or transient or could prevent or mitigate an accident after its occurrence. Both passive and active components are included.

As stated in a draft 10 CFR 50.65, "Requirements For Maintenance Programs Of Nuclear Power Plants", maintenance at nuclear power plants is the aggregate of those planned and systematic actions required to prevent the degradation or failure of, and to promptly restore the intended function of structures, systems, and components. This applies to all parts of the plant that could significantly impact safe operation, including the balance of plant (BOP). The basis for this is the fundamental principle of defense in depth that underlies all NRC regulation. Defense in depth provides for both accident prevention and accident mitigation, with principal and primary emphasis on prevention. Structures, systems, and components in the BOP, therefore, are included in the scope of equipment considered in the risk-focused maintenance process because failure of BOP equipment can initiate transients or accidents or adversely affect the course of transients or accidents.

One major purpose of the risk-focused maintenance process is to provide a systematic set of criteria, based on risk, for deciding which of the components considered in the process are to be defined as critical to risk ("risk-critical components"), and which are not. Only risk-critical components are included within the scope of the risk-focused maintenance process.

The risk-focused maintenance process addresses only a portion of the total plant maintenance program. Plant equipment receives and should continue to receive maintenance for reasons other than the risk-focused process described herein. Use of the risk-focused maintenance process should not preclude other maintenance activities the utility considers necessary for proper maintenance of its equipment.

The second major purpose of the risk-focused maintenance process is to provide criteria and guidance for establishing a reliability-focused maintenance program for the risk-critical components that accounts for the unique reliability characteristics of each component.

The risk-focused maintenance process, therefore, consists of two major steps, paralleling the two purposes described above: 1) identifying risk-critical components and 2) determining what maintenance activities are required to ensure reliable operation of the risk-critical components identified. Note that the overall process and the first step are "risk-focused"; the program for individual components is "reliability-focused".

2.3 APPROACHES TO IDENTIFICATION OF RISK-CRITICAL COMPONENTS

Figure 2-1 illustrates the top-level process for implementing a risk-focused maintenance program for a nuclear power plant. The first major step is to determine if the component is risk-critical. If a component is not risk-critical, it is not included within the purview of the overall risk-focused maintenance process. If the component is determined to be critical to risk, then it is incorporated into a reliability-focused maintenance program. Any systematic, self-consistent approach for implementing the process illustrated in Figure 2-1 is acceptable, as long as it is focused by risk and reliability considerations.

This report addresses two approaches to the first step in the risk-focused maintenance process. Both approaches begin with consideration of functions that must be performed for safe operation of the nuclear plant. They then identify major systems that provide essential safety functions, including mitigation of accidents, and the components that enable each such system to perform its safety functions. They then identify systems that provide support to the systems providing the essential safety functions, and components that enable these support systems to provide their support functions. In parallel, both approaches identify normally-operating systems and components whose failures could initiate an accident or transient which challenges safety systems.

The two approaches differ in their methods of identifying risk-critical components. One approach uses the results of a Probabilistic Risk Assessment (PRA). The other approach is

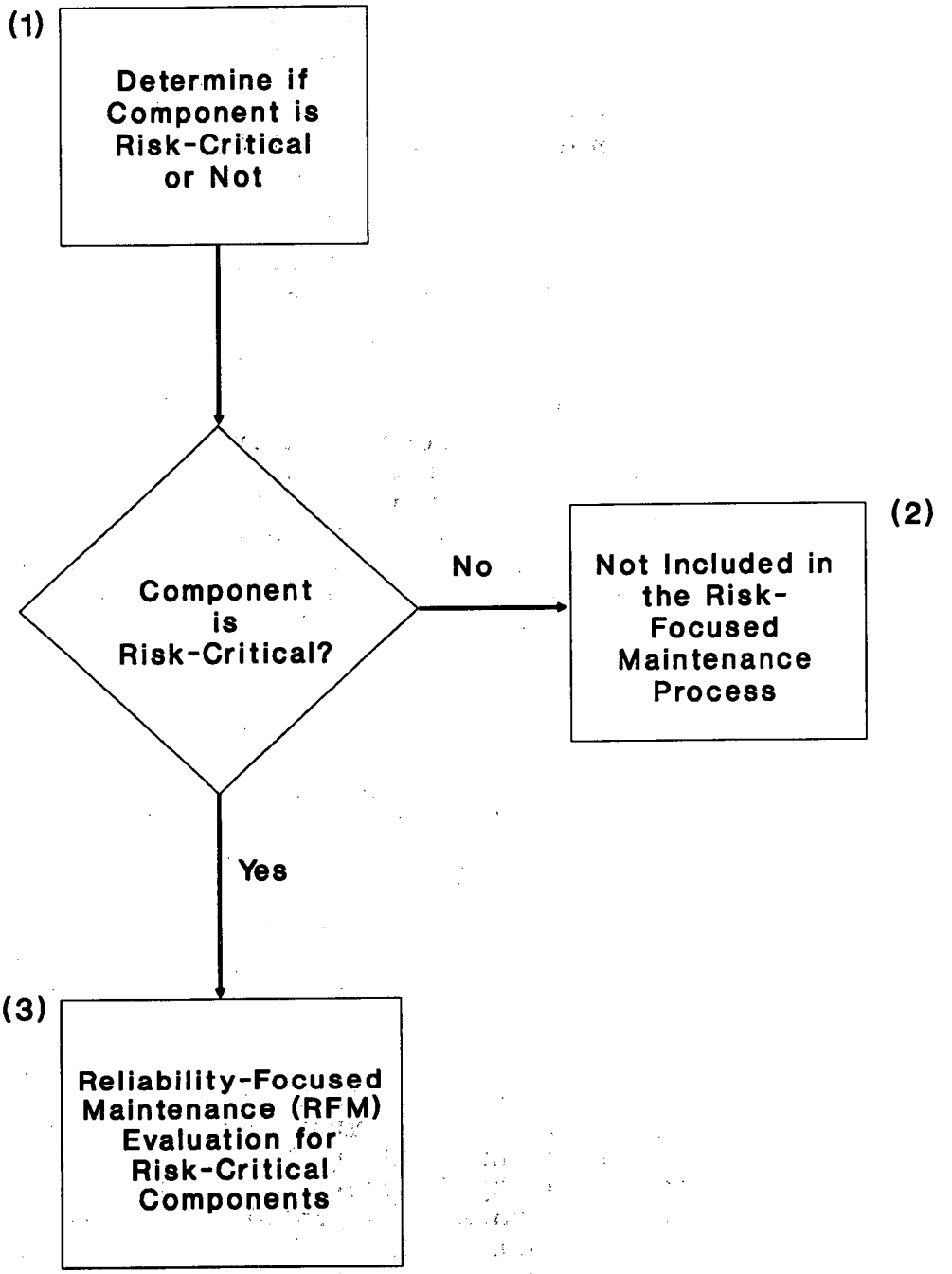


FIGURE 2-1. TOP-LEVEL RISK-FOCUSED MAINTENANCE PROCESS

appropriate for plants that do not have, or do not wish to use their PRA to identify risk-critical components. This approach is based on the methodology developed for this report which, although it does not use results of a PRA study, has a basis in PRA. Thus, the first step will be performed by, or with the assistance of, personnel familiar with PRA techniques and concepts. The two approaches to identifying risk-critical components are discussed further in Sections 3 and 4.

2.4 METHODOLOGY FOR DETERMINING MAINTENANCE ACTIVITIES REQUIRED

After the risk-critical components have been identified by one of the two approaches mentioned above, the risk-focused maintenance process uses a single methodology for the second step: determining what maintenance activities are required to ensure reliable operations of the risk-critical components identified. The methodology evaluates failure modes of risk-critical components identified in the first step and identifies maintenance activities required to defend against those failures and thus, to be incorporated into a reliability-focused maintenance program. Figure 2-2 illustrates this part of the overall process. Section 5, "Reliability-Focused Maintenance", provides a more detailed discussion of the methodology.

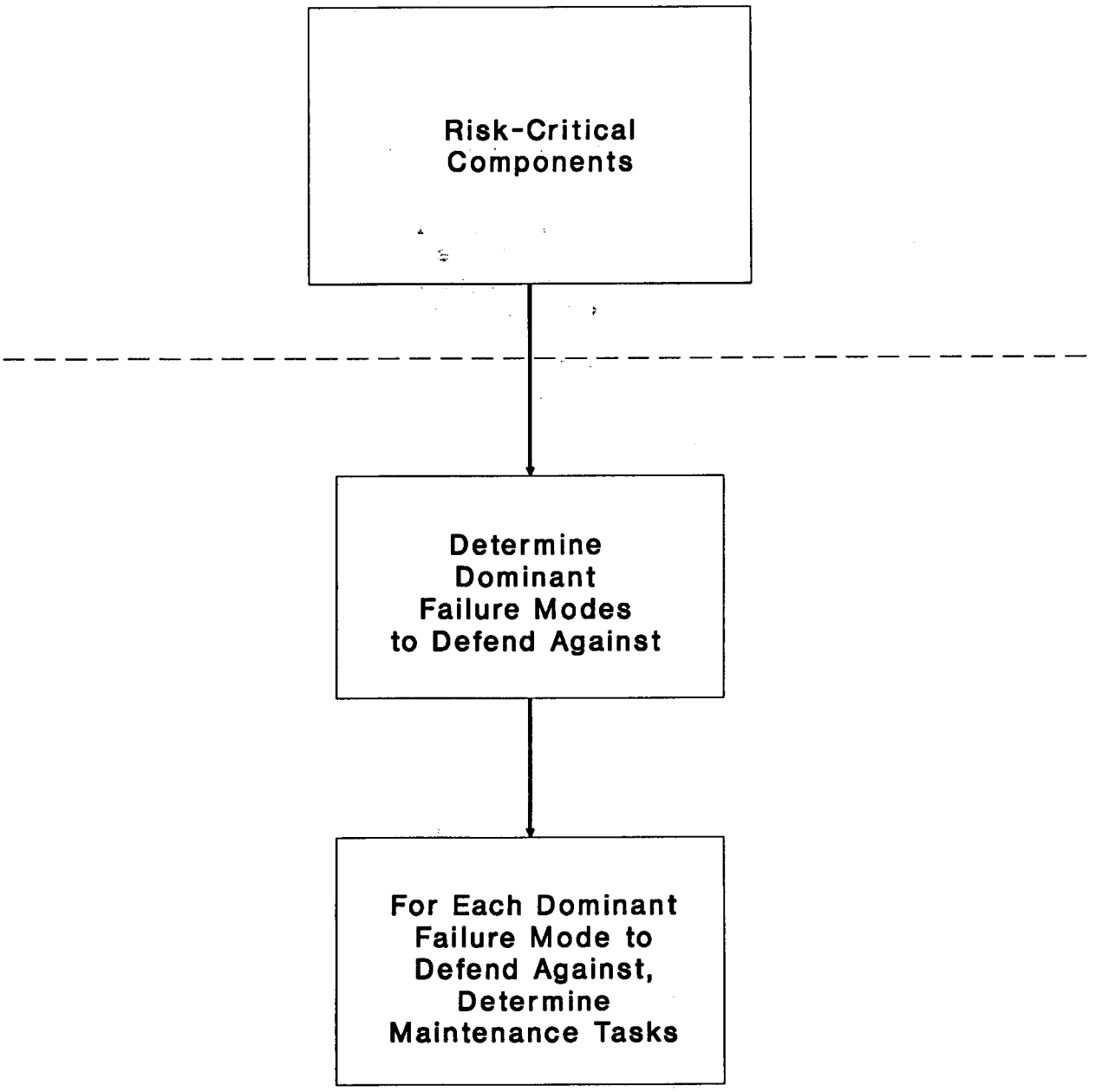


FIGURE 2-2. MAINTENANCE EVALUATION FOR RISK-CRITICAL COMPONENTS

SECTION 3

IDENTIFYING RISK-CRITICAL COMPONENTS WHEN PRA IS NOT USED

This section discusses an approach for identifying risk-critical components that does not require use of a Probabilistic Risk Analysis (PRA), and summarizes the results of a demonstration utilizing this approach. The demonstration is discussed in detail in Appendix A, "Demonstration Of Approach For Identifying Risk-Critical Components When A PRA Is Not Used".

3.1 DESCRIPTION OF APPROACH

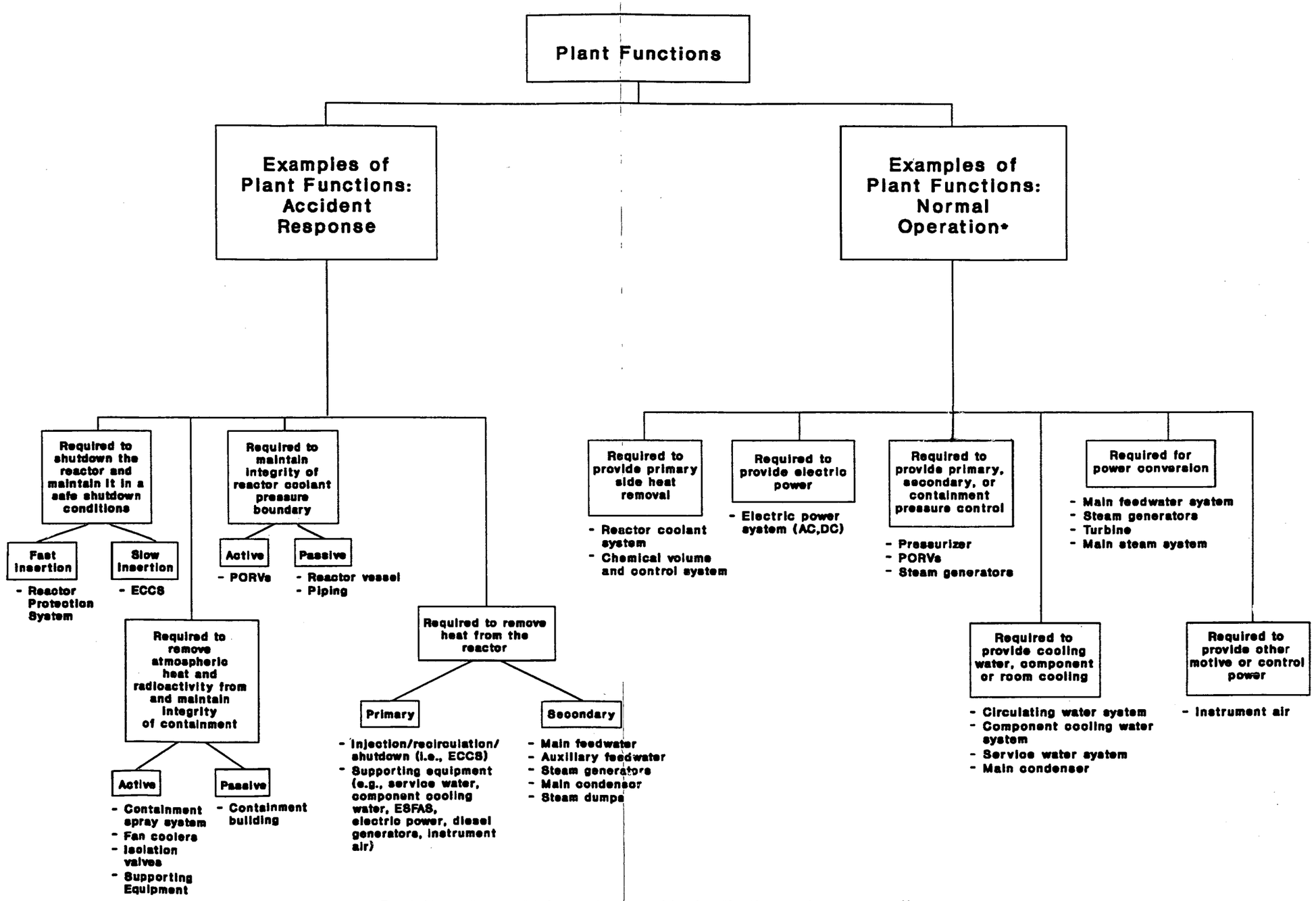
This approach is appropriate for those plants that do not have a PRA, or do not wish to use their PRA to identify risk-critical components.

The approach begins with consideration of functions that must be performed for safe operation of the nuclear plant and identification of systems performing those functions, as illustrated by the examples given in Figure 3-1. The first step in the approach identifies (1) structures, systems and components (SSCs) that are relied upon to prevent or mitigate accidents, and (2) components whose failure would cause a transient or accident requiring plant shutdown. These would include all front-line safety system components and balance of plant components whose failure would result in an accident or transient which challenges front-line safety systems. These comprise the initial set of equipment that should be under review to determine which components are risk-critical.

The next step in the approach is to identify which of those pieces of equipment are most directly involved with safe operation of the plant. The evaluation follows the logic shown on Figure 3-2. Components that have any of the characteristics shown on Figure 3-2 are designated as risk-critical components.

The next step in the approach is to add to the components identified above any components that are needed to support any component surviving the screen represented by the logic shown in Figure 3-2. This step is summarized in Figure 3-3.

Balance of plant equipment whose failure would result in an accident or transient should be considered risk-critical. However, only the most likely BOP component failures, and the ones whose failure would have the largest consequences, need be designated as risk-critical components. Similarly, components in systems that support risk-critical components should be considered as risk-critical. As with BOP components, only those support system components that fail most often and those whose failure is most consequential need be designated as risk-critical.



• Deviations from which result in accident initiation and safety challenges

FIGURE 3-1. NON-PRA PROCESS: FIRST TIER DETERMINATION OF PLANT FUNCTIONS AT THE PLANT AND SYSTEM OR COMPONENT LEVEL

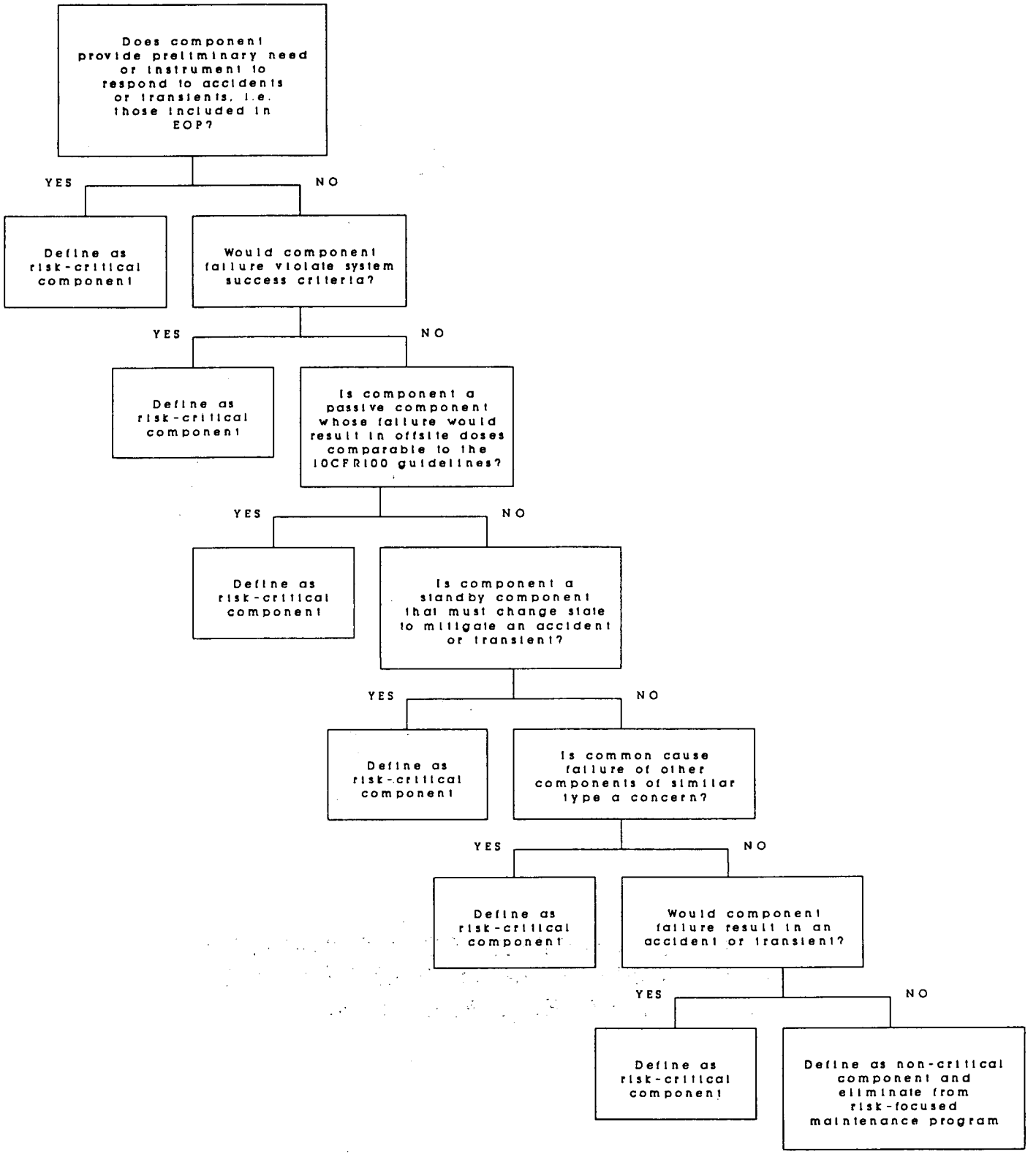


FIGURE 3-2. SECOND-TIER EQUIPMENT EVALUATION PROCESS: NON-PRA EVALUATION OF RISK-CRITICAL EQUIPMENT

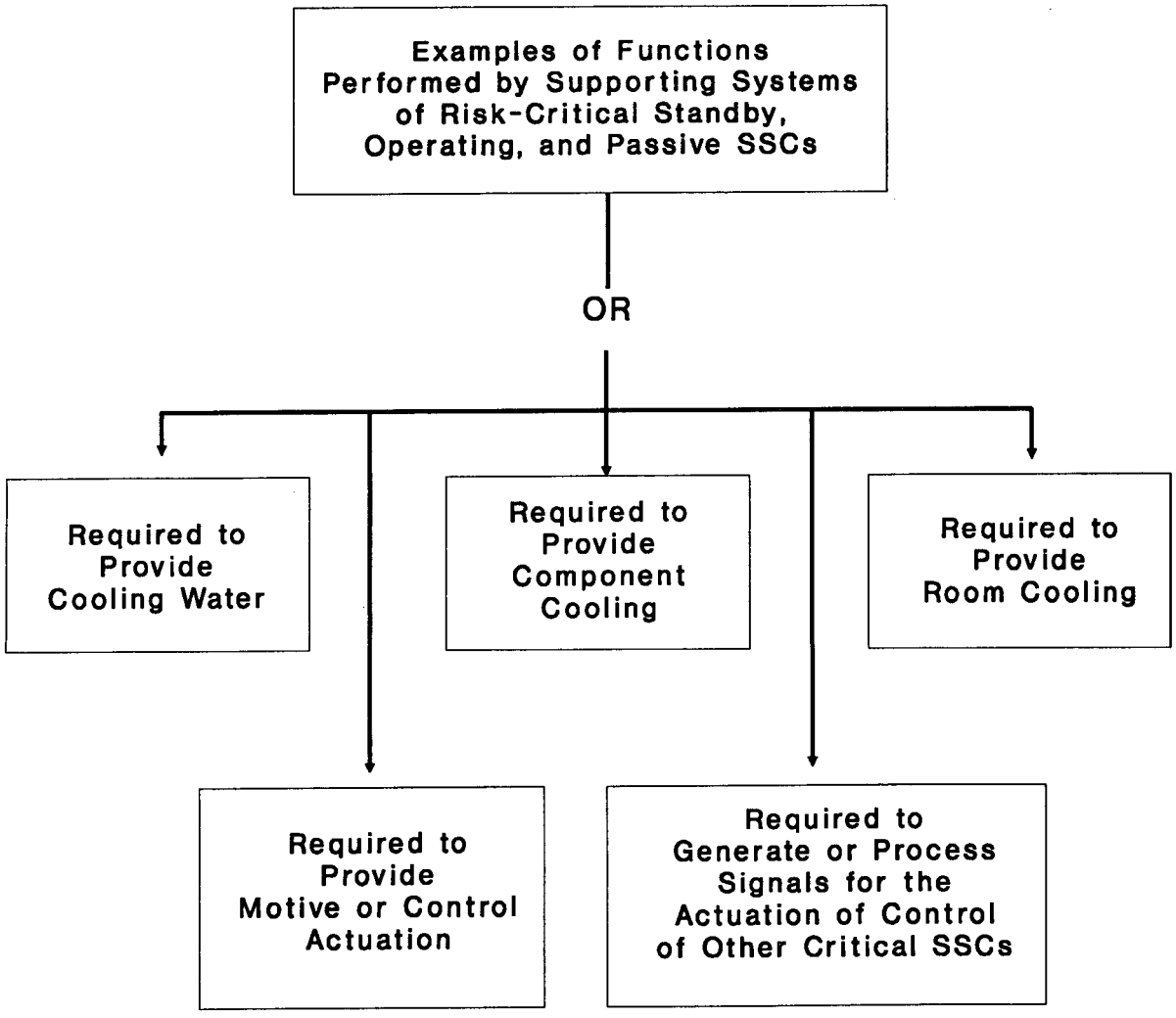


FIGURE 3-3. EVALUATION OF SUPPORT EQUIPMENT FOR RISK-CRITICAL STANDBY, OPERATING AND PASSIVE SSCs (NON-PRA BASED EVALUATION)

Finally, passive equipment whose failure would violate Final Safety Analysis Report (FSAR) success criteria (see Section 6, "Glossary Of Terms", for definition) or could result in offsite doses comparable to 10CFR100, "Reactor Site Criteria", would also be designated as risk-critical. The determination of risk-critical passive components should center on the identification of failure modes that can, or will, impact safety. Risk-critical passive components, like active components, can be categorized by safety impact on either accident initiation or accident mitigation. If failure of a component could initiate an accident or if the component is required to mitigate consequences of any accident, given that it has occurred, it should be considered a risk-critical component.

Figure 3-4 summarizes the types of equipment that would be included as risk-critical components, using the non-PRA approach described above. Major front-line safety system active components that must change state to respond to an accident or transient would be included, as well as equipment that has single failure modes that would fail a safety function. Front-line safety system active components for which there could be common cause concerns (e.g., containment isolation valves) would also be included.

3.2 DEMONSTRATION OF APPROACH

The methodology developed for determining risk-critical components without using a PRA was applied to a PWR. This demonstration included:

1) the determination of components which are critical to the prevention or mitigation of an accident,

2) the identification of potentially dominant initiators of accidents specific to the cooperating PWR plant, and

3) the determination of candidate risk-critical passive components.

The process for determining risk-critical components for initiators was illustrated in the PRA approach demonstration and was not repeated for the demonstration involving the PWR plant.

Application of the developed criteria was generally straightforward for the determination of active components (i.e., non-passive, normally operating or standby components). First, front-line systems were reviewed one at a time, using the following steps:

1) the function of the system was verified as being important to the prevention or mitigation of an accident or to the support of important systems or components,

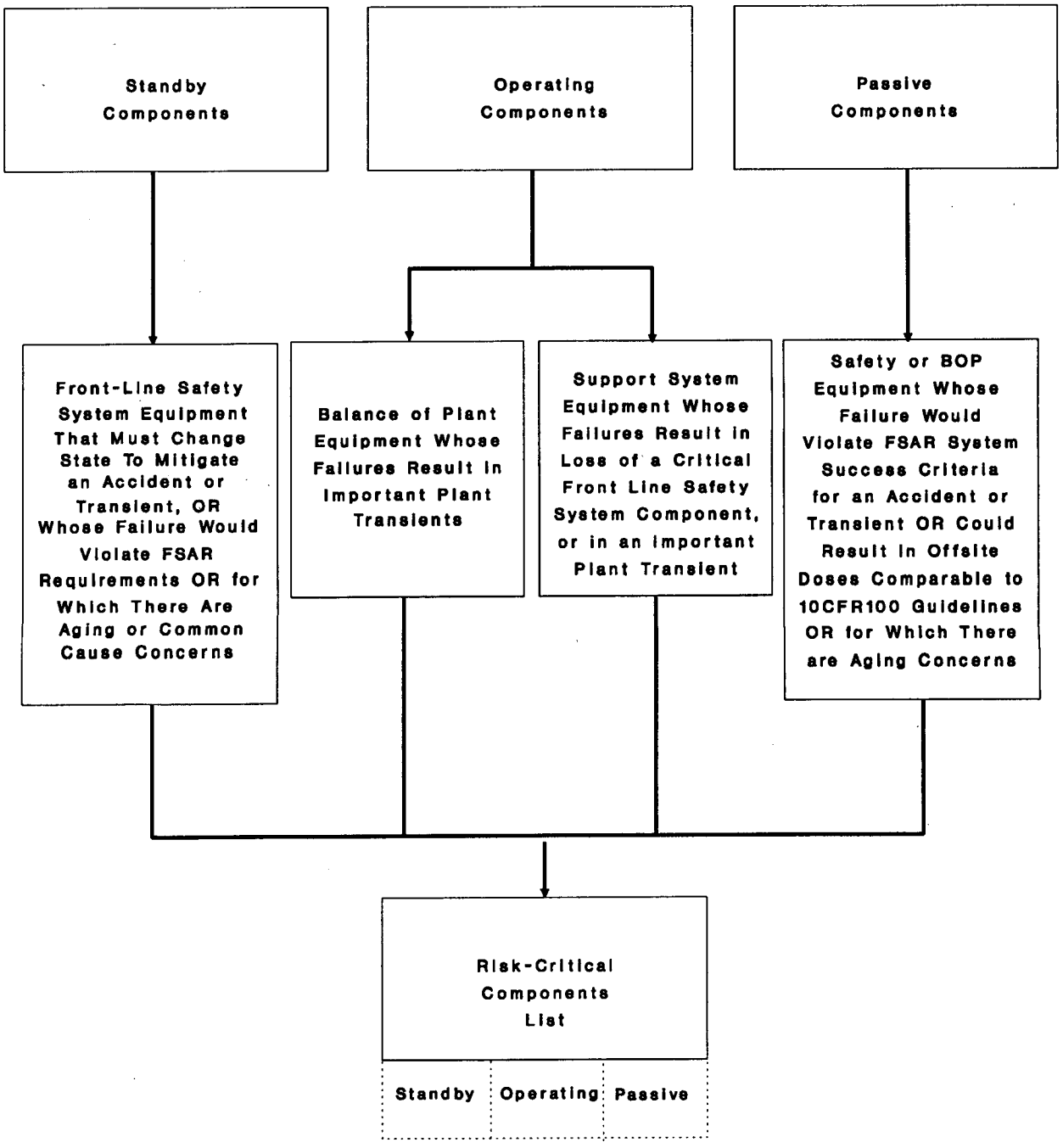


FIGURE 3-4. SUMMARY OF COMPONENTS IN RISK-CRITICAL COMPONENTS LIST

2) the criteria developed for the non-PRA approach were applied in the review of the system description and drawings, and

3) support systems for components identified as critical were identified, when possible and appropriate, from the description and drawings.

Some assumptions of functional importance were made, not unlike those in PRA system modeling. For instance, some miniflow lines were judged to be important for pump operational protection.

For support systems, such as cooling water systems, the developed criteria were also straightforward to apply. For the electric power system, however, the only applicable criterion was determined to be the requirement of support for other critical equipment. The FSAR load list and drawings proved to be the most useful in applying this criterion. The results obtained for this demonstration and that described above are shown in Tables A-1, A-3, and A-4 of Appendix A, "Demonstration Of Approach For Identifying Risk-Critical Components When A PRA Is Not Used".

As a result of the demonstration for passive components, it is recommended that the concerns in both Appendices A and E, which are relevant to passive components, be considered.

As was expected, the demonstration of the non-PRA approach was more time-intensive than was the demonstration of the PRA approach. However, the results obtained are expected to be representative of what a utility would obtain as a result of following the steps described in Appendix A, "Demonstration Of Approach For Identifying Risk-Critical Components When A PRA Is Not Used".

SECTION 4

IDENTIFYING RISK-CRITICAL COMPONENTS WHEN A PRA IS USED

This section discusses an approach for identifying risk-critical components using a Probabilistic Risk Assessment (PRA), and summarizes the results of a demonstration of this method. The demonstration is discussed in detail in Appendix B, "Demonstration Of PRA Approach For Determining Risk-Critical Components".

4.1 DESCRIPTION OF APPROACH

This approach is appropriate for those plants that have a PRA, or wish to perform a PRA as a basis for identifying risk-critical components.

An acceptable approach for identifying risk-critical components that is based on using a Level I PRA is illustrated in Figure 4-1. Note that PRA takes function into account inherently -- it is a logical process for identifying components whose failure to function would contribute to a core melt.

In order to identify risk-critical components from a PRA's accident sequences, the first step in this approach is to choose a fraction of the core melt frequency that represents the most likely accident scenarios (e.g., choose the top ninety percent as far as likelihood of occurrence is concerned). This selection can be based upon the fraction of core melt frequency results reported in existing PRAs or the fraction recommended for the Individual Plant Examination (IPE) submittal. Another possible consideration may be related to natural breaks in the rankings of cutsets. The next step in this approach is to identify the components whose failure modes are represented in this set of accident scenarios. These components are considered to be risk-critical components. Passive components which satisfy the criteria described previously for passive components in the non-PRA approach (Section 3) should also be identified. In addition, any standby components for which aging or common cause failure is a concern, either from plant-specific or industry experience, should be added to the list of risk-critical components.

In order to identify risk-critical components from accident sequences, only the most likely accident sequences are considered. The initiating events associated with those sequences are then identified. Finally, all BOP or other equipment having failure modes that could result in these transients or accidents are identified. The components experiencing the most frequent failures for each of the "dominant" initiating events are kept as risk-critical components.

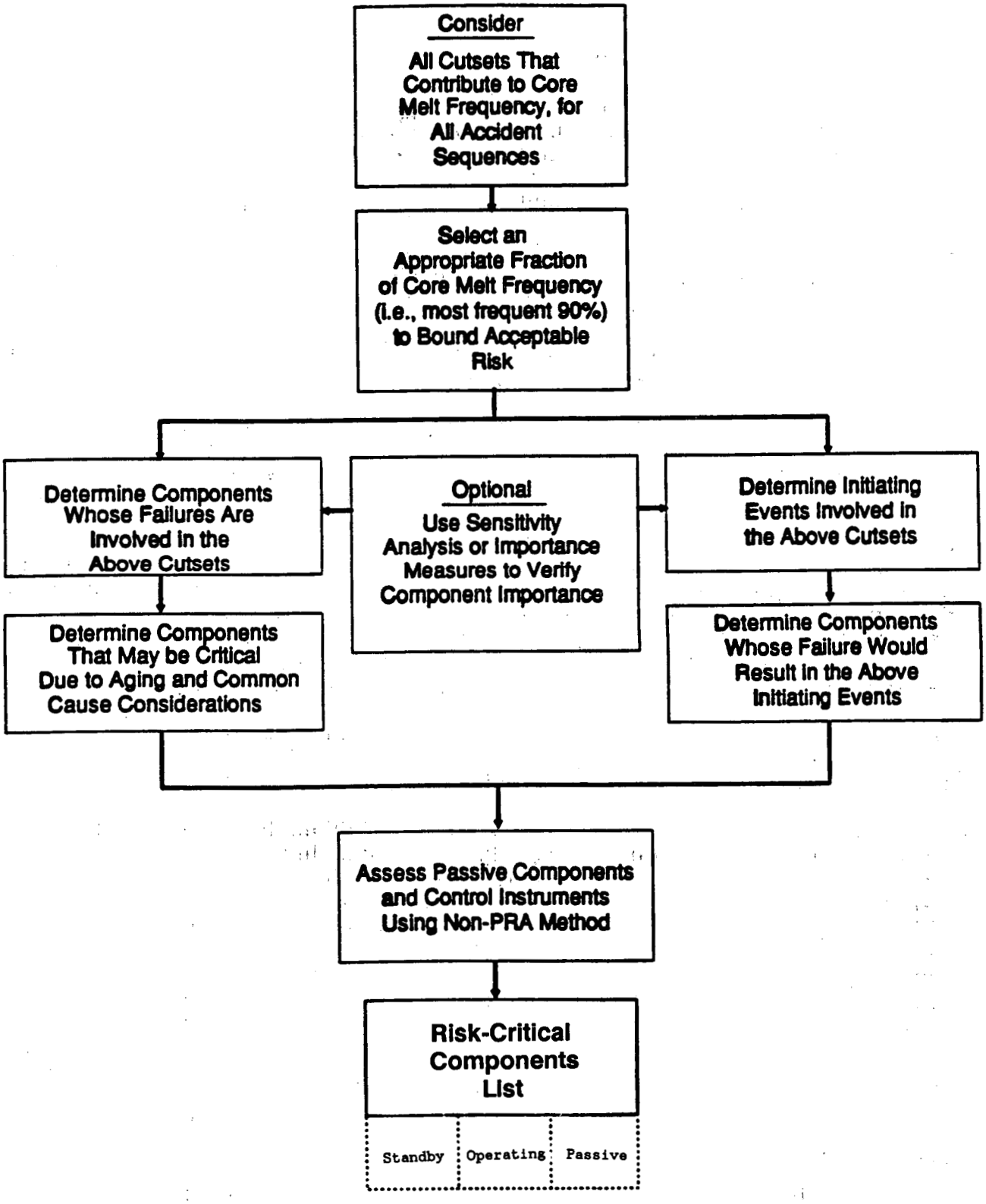


FIGURE 4-1. PRA PROCESS FOR RISK-CRITICAL COMPONENT DETERMINATION

This completes the criteria and considerations for a PRA-based identification of risk-critical components. Variations to this approach are acceptable. For instance, instead of choosing the initiating events and components whose failure modes appear in a top percentage of the cutsets, an acceptable approach would be to use importance measures or sensitivity analysis to accomplish this.

4.2 DEMONSTRATION OF APPROACH

A completed probabilistic risk assessment (PRA) for a BWR plant was used for this demonstration of the determination of risk-critical components when a PRA is available. The demonstration included:

- the determination of risk-critical components from the accident sequences represented in the PRA,
- the determination of important initiators of accidents from the PRA, and
- the determination of risk-critical components for the "Loss of Feedwater" initiator for the BWR plant.

The determination of risk-critical components for other initiators is expected to involve steps similar to those performed in this demonstration. Also, risk-critical passive components were not determined in this demonstration; the same methodology as is applied in the non-PRA approach for risk-critical component determination would be used for a plant which uses their PRA.

The methodology developed for determining risk-critical components from a PRA was straightforwardly applied to the PRA results which the cooperating utility provided SAIC.

The results of this process are shown in Tables B-2, "Risk-Critical Active Components Identified By PRA Accident Sequences", B-3, "Risk-Critical Electrical Components Identified By PRA, By Component Type", and B-4, "Risk-Critical Components Identified By PRA, By System", of Appendix B, "Demonstration Of PRA Approach For Determining Risk-Critical Components". One complication in the process of identifying risk-critical electrical components from this particular PRA was the inability to match up some components (e.g., relays, contact pairs, fuses, etc.) with specific risk-critical equipment (e.g., pumps, MOVS, etc.) due to the lack of notation in the master data file. This problem could be solved by consultation with the PRA staff at the cooperating utility. However, SAIC recommends that the criticality of these components be verified in the risk-focused maintenance process.

Overall, the performance of this demonstration went as planned. In reviewing the contributors to the accident sequences for this PRA, it was evident that the majority of the modules and their associated component failure modes could have been captured by

using only 75% of the PRA results. However, SAIC elected to report all the results available to us. SAIC anticipates that application of this PRA approach to other PRAs will involve similar efforts and results.

REFERENCE

4-1. Stetson, et.al., "Analysis of Reactor Trips Originating in Balance of Plant Systems", prepared for U.S. NRC, SAIC-89/1140, September 1989.

SECTION 5

RELIABILITY-FOCUSED MAINTENANCE

This section describes the methodology for developing a reliability-focused maintenance program for risk-critical components, and presents summaries of three demonstrations of this process: for a standby safety system (active) component; for a normally operating system (main feedwater) component; and for a passive component. Those demonstrations are discussed in detail in Appendices C, "Demonstration Of Reliability-Focused Maintenance For Standby Components", D, "Demonstration of Reliability-Focused Maintenance For A Normally Operating System", and E, "Demonstration Of Reliability-Focused Maintenance For Passive Components", respectively.

5.1 DESCRIPTION OF METHODOLOGY

This methodology is appropriate for establishing a reliability-focused maintenance program for risk-critical components identified by either the PRA or non-PRA approaches described in the preceding sections.

Establishing a reliability-focused maintenance program for a risk-critical component involves determining the preventive or predictive maintenance actions (e.g., surveillance, condition monitoring, overhaul) or other maintenance-related activities such as redesign, or reconfiguration, which are responsive to the reliability needs of that component (i.e., a reliability-focused maintenance program akin to Reliability-Centered Maintenance (RCM)). Information on RCM techniques may be found in References 5-1, 5-2, and 5-3, respectively.

Figure 5-1 indicates, as guidance, the two steps that should be addressed by an acceptable reliability-focused program for a risk-critical component.

The first step is to determine the dominant component failure modes that should be defended against. The second step is to determine maintenance activities that will defend against those dominant failure modes. Methodologies for completing each step are discussed below. Other methodologies would be acceptable, as long as they account for the reliability characteristics of a component and develop a maintenance program to defend against the most important failure modes of the component.

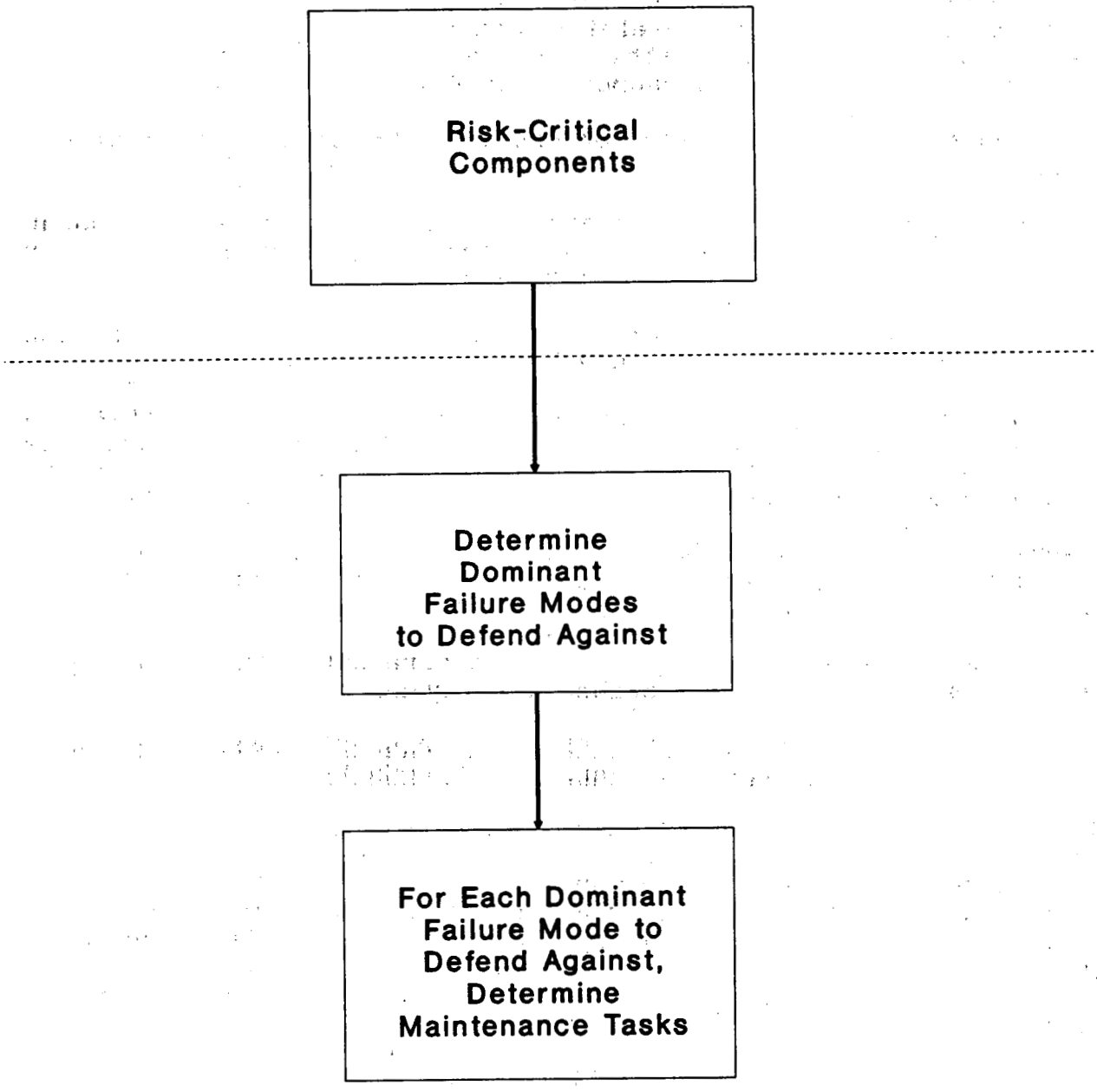


FIGURE 5-1. MAINTENANCE EVALUATION FOR RISK-CRITICAL COMPONENTS

5.2 DETERMINE DOMINANT COMPONENT FAILURE MODES

Figure 5-2 shows an expanded version of a reliability-focused process for identifying the most important component failure modes. Three assessment paths are shown in that figure: "Identify Risk-Critical Pieceparts Using Qualitative, Analytical Methods"; "Identify Risk-Critical Pieceparts from Failure History", and; "Identify Existing Maintenance-Related Activities and Requirements". These three assessment paths are denoted Assessment Path A, Assessment Path B, and Assessment Path C, respectively.

Assessment Paths A and B are options for identifying the dominant failure modes.

- Assessment Path A would be used for complex equipment such as diesel generator systems or feedwater systems, or when failure history data are not available.

- Assessment Path B would be used for less complex equipment when failure history data is available.

Both of the above paths should be used to provide substantiating evaluations of failure modes to defend against, when this is appropriate. Identifying the dominant failure modes is assumed to be synonymous with identifying the risk-critical pieceparts.

Assessment Path C should be done for each risk-critical component (after or in parallel with Assessment Path A or B) and is not to be considered optional.

The three Assessment Paths are shown in more detail in Figure 5-3. Each assessment path is described briefly below.

5.2.1 Assessment Path A: Identify Risk-Critical Pieceparts Using Qualitative, Analytical Methods

The activities using qualitative, analytical methods to identify dominant failure modes of the risk-critical components are summarized in the left-most column of Figure 5-3. In this option, a qualitative analytical reliability tool such as fault tree, Failure Modes and Effects Analysis (FMEA), or reliability block diagram is used to identify pieceparts of risk-critical components whose failures are of the types shown in the large box in the middle of Path A of Figure 5-3, namely:

- Single piecepart failures that fail the component's function and that are likely to occur

- Latent piecepart failures that are not detectable through ordinary component demand testing

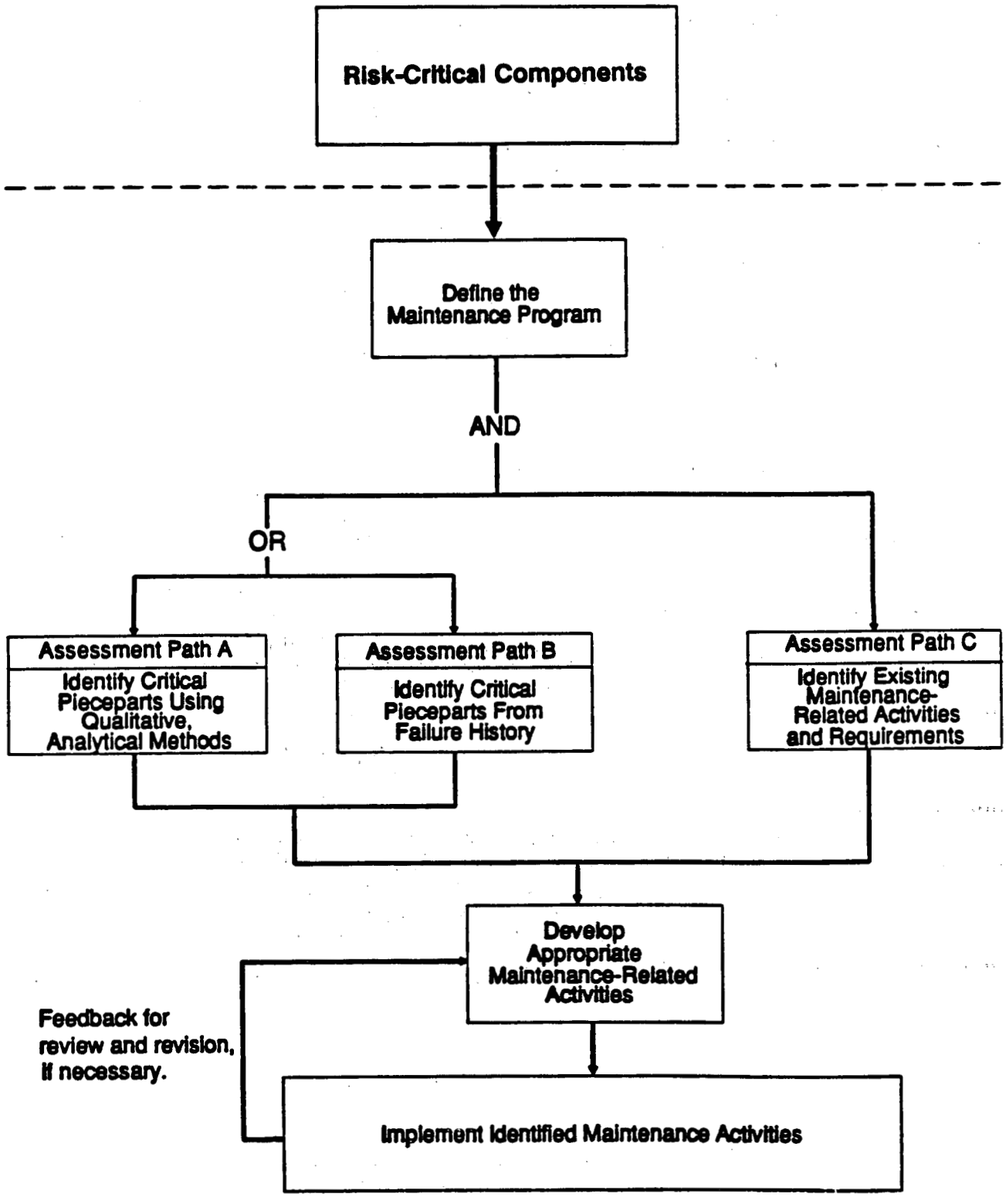


FIGURE 5-2. EVALUATION PROCESS FOR OPERATING AND STANDBY EQUIPMENT

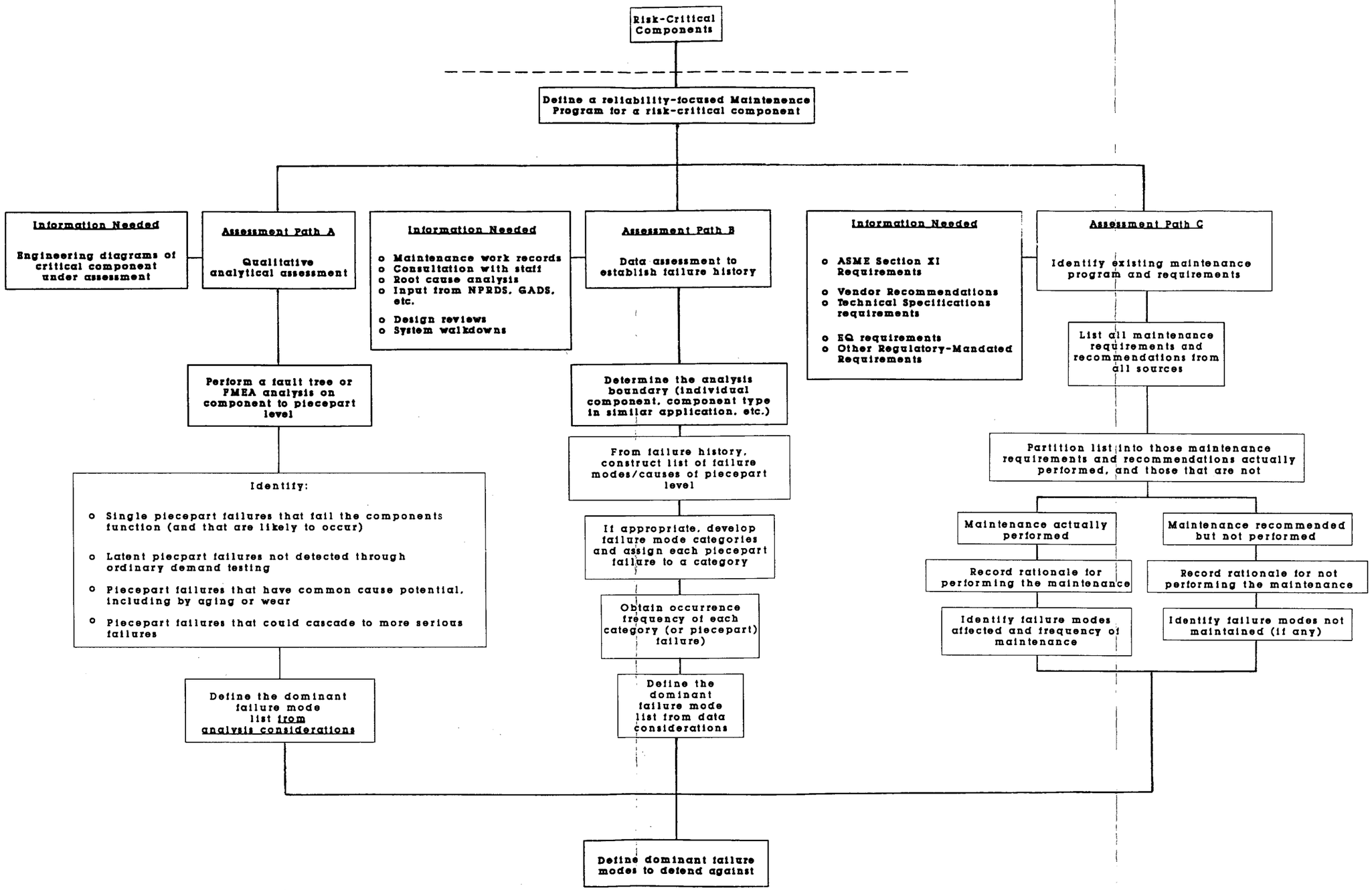


FIGURE 5-3. SUMMARY OF PROCESS FOR DETERMINING DOMINANT FAILURE MODES OF RISK-CRITICAL COMPONENTS

- Piecepart failures that, though internally redundant, have common cause potential

- Piecepart failures that have large consequences in terms of repair resources required, or that could cascade to more serious failures. The piecepart failures that will be defended against by preventive/predictive maintenance or by other means should be chosen from this set.

5.2.2 Assessment Path B: Data Assessment to Establish Failure History

A failure history assessment option for determining dominant failure modes of the risk-critical components is summarized in the center column of Figure 5-3. Since a reasonably long failure history is necessary for most components to determine the dominant failure modes from failure and repair data, it may be useful to combine components into categories that would allow pooling, or mixing of the failure histories from several components. One acceptable option would be to combine the failure histories of components of the same type in the same environment, such as large MOV's that see borated water environments. Thus, the first step in this option is to develop the analysis boundary in terms of categories of equipment whose repair and failure data would be pooled.

The next step in this option is to construct the list of failure modes found in the failure data. This should be accomplished in terms of piecepart failures using, if available, piecepart failure cause data. If piecepart failure cause data is not available, the list should be constructed by major piecepart failure (e.g., "valve driver", "valve gate binding", etc).

The occurrence frequency of each category is then computed, and the categories are ranked by occurrence frequency, with the most frequently occurring piecepart failures indicated as the prime candidates for inclusion as the dominant failure modes.

5.2.3 Assessment Path C: Identify Existing Maintenance Program and Requirements

The steps to assess existing maintenance requirements and recommendations for each risk-critical component are summarized in the right-most column of Figure 5-3. Recall that this assessment is to be conducted after, or in parallel with, the assessment in Path A or B; it is not considered an option.

In overview, the suggested assessment process is to collect and review all maintenance requirements and recommendations for the component from all relevant sources, and then partition these into maintenance actions that are part of the existing maintenance plan for the component, and those that are not being performed.

Rationales are developed for both sets of maintenance actions. That is, a rationale is developed for each maintenance act that is currently being performed; and a rationale is developed to explain why each recommended maintenance act that is currently not being performed is in the "not performed" category. This explicit set of steps could serve as a starting point for the assessment of maintenance needs for the component.

The dominant failure modes which should be defended against and for which maintenance strategies should be devised will be those identified in assessment path C, plus those identified using a reliability assessment similar to assessment paths A and/or B.

5.3 DETERMINE MAINTENANCE FOR DOMINANT FAILURE MODES

Figure 5-4 summarizes the process for determining risk-critical component maintenance. The process of determining effective maintenance to defend against the dominant failure modes of a component is largely one of engineering judgement. However, there are bookkeeping tools that can aid systematic completion of this task. Table 5-1 represents one configuration that could assist the process of determining effective maintenance. All dominant failure modes for a single risk-critical component are listed in the left-most column of the matrix, usually as individual piecepart failures. Succeeding columns, from left to right, list:

- Consequences of each of these piecepart failures in terms of resources for repair, impacts on risk, impacts on technical specifications (if any), potential for cascading or common cause failure, etc.
- The estimated occurrence frequency for each piecepart failure, estimated either from historical failure data, or as a category such as high, medium, or low.
- Instrumentation, if any, that would provide an indication that the piecepart has failed or is likely to fail.
- Whether the piecepart failure is latent or announced.
- Potential maintenance defenses such as preventive or predictive maintenance, surveillance, etc. that could be used to detect the piecepart failure or a precursor to piecepart failure or prevent the failure.

The last column represents a final assessment as to whether or not the failure mode will be defended against.

5.4 DEMONSTRATION FOR STANDBY SAFETY COMPONENTS

For the purposes of this demonstration, an existing Reliability-Centered Maintenance (RCM) study, which was completed approximately

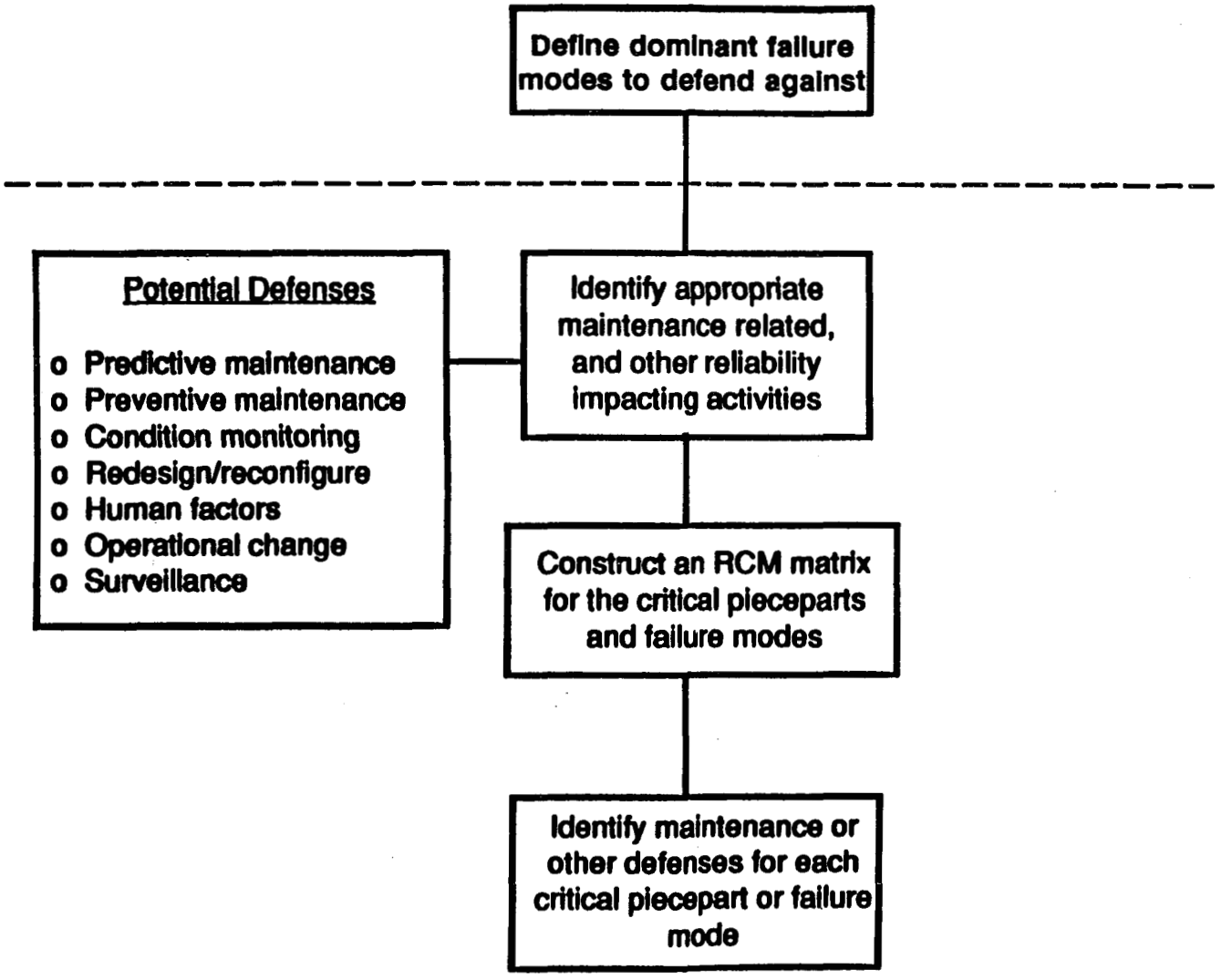


FIGURE 5-4. PROCESS FOR DETERMINING MAINTENANCE FOR DOMINANT FAILURE MODES OF CRITICAL COMPONENTS

TABLE 5-1. CRITICAL FAILURE MODE DETECTION MATRIX

(RCM Matrix)

Critical Failure Mode	Failure Mode Impacts			Occurrence Frequency	Instrumentation	Latent or Announced	Potential Detection or Defenses	Critical Failure Mode?
	Repair Outage Time	Impact on Risk	Impact on LCO's					
fM1								Yes
fM2								Yes
.								.
.								.
.								.
.								.
.								.
.								.
fMn								No

a year prior to the start of the Risk-Focused Maintenance project, was used. That study identified important components of the Auxiliary Feedwater (AF) System. The methodology in that study was compared with the methodology described in this report. There appears to be considerable similarity between the two approaches.

Differences in goals (RCM attempts to optimize maintenance from both safety and economic standpoints; the methodology in this report considers safety only) and differences in determination of component "criticality" leads to some differences in respective lists of important or risk-critical components.

Despite the differences, the results of the RCM study determination of important components were considered acceptable for the reliability-focused maintenance process. A qualitative analysis, rather than the quantitative analysis indicated in Path B of Figure 5-3, was performed in this demonstration. However, either quantitative or qualitative failure history analysis may be appropriate and, in some cases, sparse data may preclude the performance of quantitative analysis.

Comparison of the RCM approach and the reliability-focused maintenance approach showed that the PRA-based boundary definitions used in the latter have the advantages of providing a logical basis for minimizing the possibility of "missing" components and of providing expanded component boundaries that may be useful in identifying failure drivers for risk-critical components having a relatively high corrective maintenance load.

From the utility's perspective, the results of this study indicate that, through the application of reliability-centered maintenance, preventive maintenance man-hours can be more efficiently optimized. Several maintenance tasks were identified that were recommended to be deleted, modified, or changed to condition-directed and one time-directed task was recommended to be added. Overall, the total time-directed preventive maintenance workload on the AF system would be changed from 67 time-directed tasks to 61, and the number of condition-directed preventive maintenance tasks would be increased from zero to seven. For the purposes of reliability-focused maintenance, however, only 11 risk-critical components and their associated tasks were impacted (i.e., modified). Due to the redundancy in system design, these 11 tasks represent only 3 types of component tasks.

5.5 DEMONSTRATION FOR NORMALLY OPERATING COMPONENTS

For the purposes of this demonstration, a Reliability-Centered Maintenance (RCM) study was used which was performed for the Feedwater (FW) System in a BWR plant at the request of the cooperating utility. There were some significant differences between lists of critical components developed from this RCM study and those developed by a PRA.

The differences are due primarily to the fact that the RCM study was performed for the normally operating function of the FW system rather than for the specific function of the FW system which must be performed in response to an accident. Although the RCM study approach is appropriate for finding the dominant causes of the "Loss of Feedwater" initiating event, the system function definition used in the RCM study results in the identification of several components which do not serve any useful function in the FW system response to accidents (e.g., zinc injection pumps). (In addition, the utility made use of a PRA modeling technique of incorporating the lube oil pumps within the main feedwater pumps' component boundaries. Hence, lube oil pumps were not identified as risk-critical components.)

In results of this particular FW RCM study, the overlap with risk-critical components from Appendix A, "Demonstration Of Approach For Identifying Risk-Critical Components When A PRA Is Not Used", is sufficient for the purposes of risk-focused maintenance. However, it is recommended that the appropriateness of using traditional RCM studies for normally operating systems be justified by a similar comparison of "critical" and risk-critical component lists or by some other means.

Like the system analyzed in Appendix C, "Demonstration Of Reliability-Focused Maintenance For Standby Components", the Feedwater System (FW) is a safety-related system subject to technical specifications. The effect of proper preventive and corrective maintenance on this system has a direct impact on plant operation and safety. Therefore, the benefits derived from reliability-centered maintenance studies on such systems are quite subtle, and recommended maintenance activity changes are not easily undertaken when changes to technical specification or regulatory commitments are also considered.

From the utility's perspective, the results of the RCM study, like the one discussed in Section 5.4 above, indicate that preventive maintenance man-hours can be more efficiently optimized through application of reliability-centered maintenance. Several maintenance tasks were identified that were recommended to be deleted, modified, or changed to condition-directed. Three time-directed tasks were recommended to be added. Overall, if the recommendations noted in the RCM study are accepted, the total time-directed preventive maintenance workload on the FW system would be changed from 165 time-directed tasks to 127. The number of condition-directed preventive maintenance tasks would be increased from zero to three. For the purposes of <u>risk-focused</u> maintenance, however, only the three main feedwater pumps were impacted, representing only one <u>type</u> of component task which was recommended to be modified. Only 39 of the original 165 tasks analyzed by the RCM study were related to risk-critical components identified in Appendix B, "Demonstration Of PRA Approach For Determining Risk-Critical Components". Table D-5, "FW System RCM

Recommendations: System-Wide And For Risk-Critical Components Only", summarizes the recommendations of the FW RCM study and contrasts these results for the entire system with those which are applicable to identified risk-critical components only.

5.6 DEMONSTRATION FOR PASSIVE COMPONENTS

Identification of risk-critical passive components and the decision to include such risk-critical components in a Reliability Focused Maintenance (RFM) program requires a different set of procedures than that for active components. Unless they are subject to a continuing monitoring program, passive components rarely "announce" a failure. When a pipe leaks, a vessel fractures, or a seal ruptures there is usually very little warning. Further, the types of maintenance practices available are limited. Pipes are not lubricated, there are no bearings to replace, electrical connections cannot be replaced, and so forth.

Thus, there is an inherently different selection process and rationale for the inclusion or exclusion of passive components. Selection involves consideration of both the risk of a passive component failure and the effectiveness of maintenance activities that may be applied to that component.

Appendix E, "Demonstration Of Reliability-Focused Maintenance For Passive Components", discusses application of procedures for identifying risk-critical passive components in the Component Cooling Water System (CCWS) at an operating nuclear plant. The Service Water System (SWS), a support system to the CCWS, was also examined.

Risk-critical passive components are shown in Table E-1, "Risk-Critical Components For RCM". These components can fail in one of three credible modes: (1) overload, (2) fatigue and fatigue-related crack growth, and (3) environmentally related failures (e.g., corrosion). Overload failures were excluded initially on the basis that there is no maintenance activity (inspection, testing, or replacement for passive components) that can guard against an overload. Since there is a continuous monitoring system (a corrosion rack) in the SWS that would detect the onset of corrosion, environmental failure modes were also excluded.

The final failure mode, fatigue, is time-dependent and non-linear. As damage accumulates, the rate of damage accumulation increases (i.e., there is an acceleration in the damage). Thus, a component that is initially in an undamaged state, and thus would not be susceptible to fatigue-related failures, would be excluded from a RFM program. Ten years later, however, it may have acquired significant damage and should be monitored or replaced (i.e., be included in an RFM program). The list of passive components to be included in an RFM program, therefore, will change with time.

Appendix E, "Demonstration Of Reliability-Focused Maintenance For Passive Components", discusses a methodology for determining whether components potentially subject to fatigue-related failures should be included in an RFM program (the methodology is applicable, in principal, to various materials and is illustrated in Appendix E for steel components). It is a conservative methodology, since it is based on analysis that predicts the time in which a measurable crack will have doubled in size (rather than when the component will have failed). Using the methodology, it is possible to determine which components should be included and to schedule RFM programs for passive components.

REFERENCES

5-1. F. S. Nowlan, et al., "Reliability Centered Maintenance", prepared by United Airlines, Report No. A066-579, December 1978.

5-2. T. G. Hook, et. al, "Application of RCM to San Onofre Units 2 and 3 Auxiliary Feedwater System", EPRI Report NP-5430, September 1987.

5-3. "Demonstration of Reliability-Centered Maintenance, Vol. 1: Project Description", (EPRI-6152), Interim Report, January 1989.

SECTION 6

GLOSSARY OF TERMS

This glossary defines certain terms, in the context in which they are used in this report.

Accident sequence: A sequence of events leading to a particular accident.

Source: "Reliability and Risk Analysis: Methods and Nuclear Power Application", Norman J. McCormick, 1981.

Active Component: A component which normally is operating or can and should change state under normal operating conditions or in response to accident conditions (e.g., pumps, valves, switches).

Source: SAIC

Aging: "The components and structures in these reactors involved a broad spectrum of materials and designs, they operate and function under different applications and environments, and they are maintained with differing practices and philosophies. Consequently, there are a variety of factors which can lead to the degradation of the functional capability of equipment. These include:

1. Natural, internal chemical or physical processes during operation;

2. External stressors (e.g., radiation, humidity, chemical, etc.) caused by the storage or operating environment;

3. Service wear, including changes in dimensions and/or relative positions of individual parts or subassemblies caused by operational cycling;

4. Excessive testing; and

5. Improper installation, application, or maintenance.

For the purpose of this discussion and throughout this report the term 'aging', represents the cumulative changes with passage of time that may occur within a component or structure because of one or more of the afore mentioned factors".

Source: U.S. Regulatory Commission, "Nuclear Plant Aging Research (NPAR) Program Plan", NUREG-1144, July 1985, Page 1-2.

Aging Mechanisms: Aging Mechanisms are the physical or chemical processes that result in aging degradation. These mechanisms include but are not limited to fatigue, crack growth, corrosion,

erosion wear, thermal embrittlement, radiation embrittlement, biological effects, creep, and shrinkage.

Source: Proposed Rule Part 54, "Requirements for Renewal of Operating Licenses for Nuclear Power Plants", 55 FR 29059, July 17, 1990.

Age-Related Degradation: Age-related degradation means a change in a system's, structure's, or component's physical or chemical properties resulting in whole or part from one or more aging mechanisms. Examples of change due to age-related degradation include changes in dimension, ductility, fatigue capacity, fracture toughness, mechanical strength, polymerization, viscosity, and dielectric strength.

Source: Proposed Rule Part 54, "Requirements for Renewal of Operating Licenses for Nuclear Power Plants", 55 FR 29059, July 17, 1990.

Basic Event: A basic fault event which requires no further development in a fault tree (i.e., the appropriate limit of resolution has been reached). In a system fault tree, basic events can be component failure modes, test and maintenance unavailabilities, human errors, etc.

Source: "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", NUREG/CR-2300, Vol. 1, January 1983.

Component: Any constituent element of a system -- structural, mechanical, electrical, hydraulic, pneumatic, magnetic, etc. In PRA usage, a component is further defined as the most basic element for which failure data is available for fault tree quantification. Examples of such components are pumps, valves, tanks, diesel generators, and buses. Synonymous with "Equipment".

Source: SAIC

Corrective Maintenance: Actions taken to restore operational capability to equipment that has failed or malfunctioned in use or is found to be incapable of performing its required functions on demand.

Source: SAIC, based on description in the latest NRC draft Reg Guide.

Critical: Generally used in this report as short-hand for "risk-critical".

Source: SAIC

Cutset: Used to mean "minimal cutset" in this report. A minimal cutset for a system is a set of system events that, if they all occur, will cause system failure, and that are not a subset of the events in any other cutset. A minimal cutset for an accident sequence is similarly defined but contains events in different systems and corresponds to the failure of the plant as a whole to respond to a particular initiating event (or accident).

Source: "Reliability and Risk Analysis: Methods and Nuclear Power Application", Norman J. McCormick, 1981.

Equipment: Synonymous with "Component".
Source: SAIC

Event Tree: Used synonymously with System (rather than containment) event tree. An event tree is an inductive logic model which is typically used in PRAs to organize and characterize potential accidents by relating mitigating system responses to identified initiating events. The objective of event tree development is to define a comprehensive set of accident sequences that encompasses the effect of all realistic and physically possible potential accidents involving the reactor core.
Source: "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", NUREG/CR-2300, Volume 1, January 1983.

Failure Mode: Consistent with usage in the PRA community, the manner in which a component can fail (e.g., for pumps: fails to start, fails to run; for valves: fails to open or fails to close).
Source: U.S. Regulatory Commission, "Fault Tree Handbook", NUREG-0492, January 1981

Frequency: As most commonly used in this report, the number per unit time of occurrences of severe nuclear power plant accidents which can produce a core melt (i.e., core melt frequency).
Source: "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", NUREG/CR-2300, Volume 1, January 1983.

Initiating Event: In PRA, the starting point of an accident sequence.
Source: "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", NUREG/CR-2300, Volume 1, January 1983.

Maintenance: The aggregate of those functions required to minimize the degradation or failure of, and to restore the intended function of, structures, systems, and components. It includes predicting, measuring, and preventing or correcting degraded conditions due to environment and service over time, and supporting activities.
Source: Proposed 10 CFR 50.65

Passive Component: A component that cannot or should not change state under normal operating conditions or in response to accident conditions (e.g., piping, tanks, reactor vessel, heat exchangers).
Source: SAIC

Piecepart: A portion of a (risk-critical) component whose failure would cause the failure of the component as a whole. The precise definition of a "piecepart" will vary between component types,

depending upon their complexity. For instance, torque/limit switches may be appropriate "pieceparts" for motor-operated valves, while air-start systems may be appropriate "pieceparts" for diesel generators.

Source: SAIC

Periodic Maintenance: Maintenance actions scheduled to be taken routinely when a specified time has elapsed, equipment has operated for a specified time, or a specified event occurs (e.g., there is a plant shutdown or Predictive Maintenance monitoring or other Preventive Maintenance inspections show that a task should be performed).

Source: SAIC, based on description in the latest NRC draft Reg Guide.

Predictive Maintenance: Maintenance actions taken to monitor, find trends, and analyze parameters, properties and performance characteristics, or signatures associated with equipment that indicate the equipment may be approaching a state in which it may no longer be capable of performing its intended function, and to prevent the equipment reaching that state when it is intended to be in use or to be immediately available for use.

Source: SAIC, based on description in the latest NRC draft Reg Guide.

Preventive Maintenance: Maintenance actions taken to avoid failures or malfunctions in periods in which equipment is intended to be in use or to be immediately available for use. Preventive maintenance includes predictive and periodic maintenance.

Source: SAIC, based on description in the latest NRC draft Reg Guide.

Reliability Characteristic: An aspect of a component which influences the component's contribution to system reliability, or unreliability, and, therefore, probability of core melt. Such characteristics may include the component's placement in the system design (i.e., are there redundant components?), the component's function (i.e., what does it do? Does it have to change state?), the failure probability of the component's required function, the component's operational environment, and the component's test or surveillance schedule.

Source: SAIC

Risk: The expected frequency of severe accidents which result in core damage (i.e., core melt). This is consistent with "risk" as used in Level 1 PRAs. Note that other types of risk (e.g., economic) could be used but would be inappropriate in the context of NRC's concern with safety.

Source: SAIC

Risk-Critical: Important to risk, as demonstrated by either of the two approaches given in this report or by some equivalent approach.

Source: SAIC

Success Criteria: A term used in PRAs to define the required performance of systems required to respond to an initiating event or accident. The success criteria for a system is stated in terms of required hardware (e.g., a number of required pumps, flow paths, instrument trains, or power buses) and is based upon assessments (e.g., neutronics and thermal-hydraulics calculations) of system functional capability and plant response to postulated conditions. The system success criteria is used to develop the system fault tree top event which is part of an event tree sequence.

Source: "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", NUREG/CR-2300, Volume 1, January 1983.

System: A collection of components which is configured and operated to serve some plant function, as defined by the terminology of each specific power plant (e.g., Auxiliary Feedwater System, Reactor Protection System).

Source: SAIC

System Fault Tree: A logic model for a system, constructed to determine the causes of system failure. Solution of a fault tree model consists of Boolean equations which are the minimal cutsets for the fault tree model. The probability of system failure and the relative contributions of minimal cutsets can be determined through quantification of the system fault tree model.

Source: "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", NUREG/CR-2300, Volume 1, January 1983.

Sub-System: A portion of a system for which there is usually redundant equipment and/or function (e.g., two trains of equipment, each referred to as a subsystem).

Source: SAIC

Vulnerability: Plant susceptibility to, or insufficiency of defense against, core damage (i.e., core melt) due to the frequency of severe accident initiators or the probability of failures in plant responses to such initiators.

Source: SAIC

APPENDIX A

DEMONSTRATION OF APPROACH FOR IDENTIFYING RISK-CRITICAL COMPONENTS WHEN A PRA IS NOT USED

A.1 INTRODUCTION

This appendix contains the demonstration of the non-PRA approach for the determination of risk-critical components. By way of demonstration, this approach was applied to a PWR plant of a cooperating utility.

Between this Appendix and Appendix B, "Demonstration Of PRA Approach For Determining Risk-Critical Components", the overall process for determining risk-critical components, via the non-PRA or PRA approach, is completely demonstrated. However, since the two approaches include identical tasks for determining risk-critical passive components and identifying risk-critical components which are dominant causes of accident initiators, demonstrations of the passive component and initiating event-component driver tasks are not duplicated between this Appendix and Appendix B. Hence, the demonstration in this appendix only includes:

1) the determination of active components which are risk-critical with respect to the prevention or mitigation of an accident using the non-PRA approach,

2) the determination of risk-critical passive components, and

3) the identification of potentially dominant accident initiators specific to the cooperating PWR plant.

The process for determining risk-critical components from a list of risk-critical initiators is illustrated in Appendix B, "Demonstration Of PRA Approach For Determining Risk-Critical Components".

A.2 APPROACH DESCRIPTION - DEMONSTRATION-SPECIFIC

The non-PRA approach for the determination of risk-critical components, as outlined in Section 3, "Identifying Risk-Critical Components When PRA Is Not Used", consists of two major tasks: 1) the identification of risk-critical components based upon the requirements of plant response under accident conditions and 2) the identification of risk-critical components based upon the deviations from normal plant operating conditions which initiate an accident and/or challenge plant safety systems. For each of these two tasks of the non-PRA approach, shown as separate paths in Figure 3-1, "Non-PRA Process: First-Tier Determination Of Plant Functions At The Plant And System Or Component Level", the approach

for risk-critical component determination is function-based. For the path shown on the left side of Figure 3-1, the task of risk-critical component determination is derived from concerns of what functions are required to be performed in response to an accident. The task of determining risk-critical components from accident initiators, shown as the right-hand path in Figure 3-1, involves identification of which functions, performed during the normal operation of the plant would, if interrupted, require accident response from safety systems. Figure 3-1, read from the top to bottom, also indicates that the approach for both of these major tasks involves the following progression of steps:

1) the identification of plant functions,

2) the identification of system functions, and

3) the identification of component functions.

The performance of the first two steps is similar for both the accident response and accident initiator tasks of risk-critical component determination. Following the description of a vital preliminary step, that of information gathering and plant familiarization, in Section A.2.1, these two steps common to the accident response and accident initiator tasks are discussed in Section A.2.2 and A.2.3, respectively. Discussions of the two accident response and accident initiator tasks, contained in Sections A.3 and A.4, respectively, relate to the respective strategies for accomplishing the last of the progressive steps (i.e., step #3).

A.2.1 Information Gathering and Plant Familiarization

Before the methodology developed for the non-PRA approach for risk-critical component determination can be applied, various plant information must be gathered in order to gain an understanding of plant design and operation details. This information gathering and plant familiarization task is the foundation of all succeeding steps in the non-PRA approach task and parallels the first step taken in performing a PRA. Hence, the discussion of plant familiarization and information gathering, including the list of potential information sources, which is given in the PRA Procedures Guide (Reference A-1) is equally applicable to the non-PRA approach for risk-critical component determination.

For this particular demonstration involving a PWR plant, the following sources of information regarding the operation of the plant during normal and accident conditions were used: the plant Final Safety Analysis Report (FSAR), the Nuclear Power Plant System Sourcebook, and system descriptions from the plant. In addition, the cooperating utility was available to answer questions. Because the scope of this demonstration did not allow for the same amount of information gathering as would be required for the performance

of a PRA, the available information was supplemented by general plant operating knowledge and experience gained from performing other PRA studies. If time and resources had allowed, additional sources of information would have been used, in particular, plant Emergency Operating Procedures (EOPs), controlled system drawings, and further consultations with plant personnel, particularly those who support operations.

A.2.2 Determination of Risk-Critical Plant Functions

The top-level plant functions, which are required for response to an accident or whose interruption could initiate an accident, are generally common to all nuclear power plants. Hence, generic sources of information, including existing PRAs studies, can be used for the identification of important plant functions. A combination of generic and plant-specific (i.e., FSAR) information was used in this demonstration. In practice, however, those plant functions indicated in Figure 3-1, "Non-PRA Process: First-Tier Determination Of Plant Functions At The Plant And System Or Component Level", (e.g.,"...remove heat from reactor") formed the basis of the list of plant functions for this demonstration and plant-specific information was used to verify the completeness of this list.

A.2.3 Determination of Risk-Critical Systems and Functions

Once the important plant functions are identified, the next step in applying the non-PRA approach involves determining which systems perform these critical, safety functions. Since the specifics of how general plant functions, such as those shown in Figure 3-1, are accomplished will be different for different plant types and designs, plant-specific information is required for the identification of risk-critical systems. In this demonstration, the primary sources of information used for making this determination were Chapter 15 of the plant's FSAR and conversations with utility personnel. Initial lists of plant systems, one associated with accident response and another with accident initiators, were developed for further review. System descriptions were then obtained from the utility for each of the identified systems. The system descriptions contained text, as well as drawings, which were the primary references for verifying that the system functions performed corresponded with the plant functions already identified. Based upon this verification of system function importance, both lists of systems were revised. The list of system initiators was used as input to the remainder of the accident initiator task, described in Section A.4. The list of systems necessary for accident response was compared to that used for a completed PRA study for another PWR plant. This final list consisted of only risk-critical systems for accident response which was used as input to the task discussed in Section A.3.

A.3 IDENTIFICATION OF RISK-CRITICAL COMPONENTS WITH RESPECT TO ACCIDENT RESPONSE

Once the systems which are required for accident prevention or mitigation are identified, the next step in the non-PRA approach for the accident response task is the identification of the components whose functions are vital to the success of system functions. The component functions, and therefore, risk-critical components, are identified through the use of component selection criteria, such as that given in Figure 3.2, "Second-Tier Equipment Evaluation Process: Non-PRA Evaluation Of Risk-Critical Equipment". These criteria, and the subsequently identified risk-critical components, are discussed in Sections A.3.1 and A.3.2 for active and passive components, respectively.

A.3.1 Identification of Risk-Critical Active Components

In this demonstration, application of the developed criteria was generally straightforward for the determination of risk-critical active components (i.e., non-passive, normally operating or standby components). Using system descriptions provided by the cooperating utility, each of the systems identified in the step above were reviewed for the following purposes:

1) to verify the importance of the system function to the prevention or mitigation of an accident or to the support of already identified risk-critical systems or components,

2) to identify the major paths for system success (e.g., flow path from water source to reactor vessel for safety injection systems),

3) to identify the components comprising the major flow paths,

4) to apply the criteria, shown in Figure 3-2, "Second-Tier Equipment Evaluation Process: Non-PRA Evaluation Of Risk-Critical Equipment", which embody system design and component reliability considerations, and

5) to identify, when possible and appropriate, support systems for components already determined to be risk-critical using the criteria shown in Figure 3-3, "Evaluation Of Support Equipment For Risk-Critical Standby, Operating, And Passive SSCs (Non-PRA Based Evaluation)".

The text provided in the system descriptions was most helpful to the performance of steps #1 and #5 above while the system drawings were valuable in performing all other steps. Some assumptions of functional importance were made, not unlike in PRA system modeling. For instance, some miniflow lines were judged to be important for pump operational protection but crossties between system trains were not. Also, shared components between systems (e.g., check

valves on common legs for safety injection systems) were identified in the course of tracing flow paths.

In this demonstration, a table was constructed for each system, identifying component tag numbers, component types (e.g., motor-operated Auxiliary Feedwater pump), component failure modes (e.g., fails to start/run), and impacts on system functions (e.g., loss of Auxiliary Feedwater train feeding Steam Generator #1) in order to aid in the independent review of the components identified with the above steps.

For some support systems, such as cooling water systems, the developed criteria was also straightforwardly applied as described above. For the electric power system, however, the only applicable criteria was determined to be the requirement of support for other risk-critical equipment. In addition, the Electric Power system description, class 1E load list, and single line diagrams of the plant's FSAR (Section 8.3) were the only readily available information sources adequate for this task of determining risk-critical components. More detailed drawings, which were not readily available, would have been preferable for the performance of this task. All electrical components from the breaker and motor control center (MCC) bus level and higher were included. Lower level electrical components (e.g., relays, fuses, contact pairs) associated with identified risk-critical components (e.g., motor-operated valves and pumps) were assumed to be picked up in the reliability-focused maintenance (RFM) process. The list of risk-critical, motor-driven components was compared with the FSAR's load list as a check on identification completeness. Since the FSAR does not include non-class 1E components, any such electrical components which are required to support identified risk-critical components could not be identified.

A.3.2 Identification of Risk-Critical Passive Components

The method used in this demonstration for identifying passive components paralleled that used for the identification of active components discussed above. However, due to the fact that maintenance for passive components consists primarily of monitoring, it was decided in the course of this demonstration that identified passive components be termed candidate risk-critical components. Appendix E, "Demonstration Of Reliability-Focused Maintenance For Passive Components", discusses issues concerning the inclusion of passive components on risk-critical component lists as well as their identification. It is recommended that the criteria for identifying passive components discussed in this section be used in conjunction with the concerns discussed in Appendix E.

In this demonstration, the criteria shown in Figure 3-2, "Second-Tier Equipment Evaluation Process: Non-PRA Evaluation Of Risk-Critical Equipment", (and Figure 3-4, "Evaluation Of Support

Equipment And Passive SSCs (Non-PRA Based Evaluation)") were used to identify types of passive components which are recommended to be included in a risk-critical component list. In applying these criteria for passive components, the following additional criterion seemed appropriate:

- passive components whose failure effectively fails its associated system or an associated component are identified as risk-critical candidates.

Some judgment was involved in the application of this additional criterion, as well as those others given in Figure 3-2. In this demonstration, consideration of plant age and existing monitoring programs were taken into account in applying all criteria. For instance, safety injection accumulators and steam generators were included in the list of identified passive components, due to the criterion added in this appendix, with a high level of confidence. But piping, which also satisfied this criterion, could not be definitely decided upon, as illustrated by its exclusion in identified passive component list of this Appendix and its inclusion in the list of Appendix E. The reactor vessel was also identified as a risk-critical component, due to its potential for radioactive releases upon failure. However, it is recognized that there are existing monitoring programs for both piping and the reactor vessel that are expected to be adequate for verifying the low failure probabilities of these components until later in plant life. When the plant is older there are more compelling reasons for including these components on the risk-critical component list. (See Appendix E, "Demonstration Of Reliability-Focused Maintenance For Passive Components", for further discussion and an alternative approach).

A.4 IDENTIFICATION OF POTENTIALLY DOMINANT ACCIDENT INITIATORS

The non-PRA approach for identifying plant-specific accident initiators, which are based upon system failures, involves the use of the following information: 1) the list of systems developed as described in Section A.2.3, 2) generic information, such as initiator lists for completed PRAs, NPRDS data, and References A-2 through A-4, and 3) plant-specific information, such as the plant-specific PRA initiator list, LERs, LCOs, plant incident reports, and maintenance records. Once the list of risk-critical system initiators is developed, risk-critical components can be identified using the same approach demonstrated in Appendix B.

In this demonstration, information from categories #2 and #3, as described above, were the primary sources of information. The list of systems (#1 above) was not fully developed due to the lack of system information immediately available. The cooperating plant's PRA initiator list was available but was not used in order to demonstrate this alternative approach. Using a variety of generic sources, the following non-exhaustive list of candidate system

initiators was developed (including a mixture of PWR and BWR systems and components):

- Reactor Coolant System
- Main Feedwater and Condensate Systems
- Main Steam System (e.g., MSIVs)
- Pressurizer, Steam Generator, ADVs, SRVs, steam dumps, etc.
- Main Condenser
- Service Water System
- Turbine/Generator
- Component Cooling or Circulating Water System
- Electric Power (AC and DC)
- Instrument Air
- Isolation Condenser

The plant-specific information used in this demonstration consisted 55 LERs, spanning approximately 4 years, which the utility provided. These LERS were evaluated and categorized using the initiating event categories reported in Reference A-2, shown in Table A-1. The results of the categorization were then pooled.

In order to finalize the list of system-based accident initiators, the categorized LERs and generic list of system initiators should be compared and integrated. In addition, priorities could be assigned to initiators which are required to support front-line, safety systems in response to an accident, are identified as a leading plant-specific cause of reactor trips from review of plant records (i.e., NPRDS, LERs, LCOs, etc.), or identified as a leading generic cause of reactor trips (BWR or PWR specific).

A.5 RESULTS OF APPLYING NON-PRA APPROACH FOR DETERMINING RISK-CRITICAL COMPONENTS

The results obtained for this demonstration are shown in two sets of tables. The first set corresponds with risk-critical components identified as a result of accident response requirements. The second set of results pertains to the identification of dominant accident initiators for the plant used in this demonstration.

Tables A-2 through Table A-4 list, by system and component type, risk-critical active components, candidate risk-critical passive components, and risk-critical electrical components. The results of these three tables are summarized in Table A-5. Note that, as

mentioned in the discussion above, electrical components, such as relays, fuses, etc., have not been included under the assumption that these components would be included within the boundary an associated risk-critical component in the reliability-focused maintenance (RFM) process. Also, the candidate risk-critical passive components identified are the result of one approach to the application of the developed component selection criteria. Appendix E, "Demonstration Of Reliability-Focused Maintenance For Passive Components", illustrates another approach as applied to the Component Cooling Water and Service Water systems. In addition, note that a very large (i.e., approximately half of the total) number of components were identified as risk-critical for Reactor Protection System. Due to the inherent high reliability of the components in the Reactor Protection System, it is recommended that plant-specific data be analyzed for these components in order to try to eliminate some of the more reliable of these components and to avoid making the maintenance focus upon risk-critical components too diffuse.

Table A-6 shows the results of the evaluated and categorized LERs for the cooperating utility, as described in Section A.4. As indicated in this section, this list of plant-specific, dominant transients should be supplemented by a generic list of system-based initiators. Examples of systems that should be added are: Service Water, Component Cooling Water, and the Main Condenser.

A.6 SUMMARY AND CONCLUSIONS

As was expected, the demonstration of the non-PRA approach was more time-intensive than was the demonstration of the PRA approach. In addition, due to the lack of some system information and drawings, some components, which would ordinarily be identified in the PRA approach (e.g., non-class 1E electrical components, components in the service water system which are essential for the cooling of identified risk-critical components), may not be included in the results obtained in this demonstration. However, the results obtained are expected to be representative of what a utility would obtain as a result of following the steps described in this appendix.

REFERENCES

A-1. "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", NUREG/CR-2300, Volume 1, January 1983.

A-2. McClymont, A. S. and Poehlman, B. W., "ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients", EPRI NP-2230, January 1982.

A-3. Stetson, F. T.; Gallagher, D. W.; Le, P. T.; and Ebert, M. W.; "Analysis of Reactor Trips Originating in Balance of Plant Systems", prepared for U.S. NRC, SAIC-89/1148, September 1989.

A-4. Mackowiak, D. P.; Gentillon, C. D.; and Smith, K. L.; "Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessments", prepared for U.S. NRC, NUREG/CR-3862, May 1985.

TABLE A-1

TRANSIENTS IDENTIFIED IN EPRI NP-2230

1	Loss of RCS Flow (1 Loop)
2	Uncontrolled Rod Withdrawal
3	CRDM Problems and/or Rod Drop
4	Leakage from Control Rods
5	Leakage in Primary System
6	Low Pressurizer Pressure
7	Pressurizer Leakage
8	High Pressurizer Pressure
9	Inadvertent Safety Injection Signal
10	Containment Pressure Problems
11	CVCS Malfunction-Boron Dilution
12	Pressure/Temperature/Power Imbalance - Rod Position Error
13	Startup of Inactive Coolant Pump
14	Total Loss of RCS Flow
15	Loss or Reduction in Feedwater Flow (1 Loop)
16	Total Loss of Feedwater Flow (All Loops)
17	Full or Partial Closure of MSIV (1 Loop)
18	Closure of All MSIV
19	Increase in Feedwater Flow (1 Loop)
20	Increase in Feedwater Flow (All Loops)
21	Feedwater Flow Instability - Operator Error
22	Feedwater Flow Instability - Misc. Mechanical Causes
23	Loss of Condensate Pump (1 Loop)
24	Loss of Condensate Pumps (All Loops)
25	Loss of Condenser Vacuum
26	Steam Generator Leakage
27	Condenser Leakage
	(Continued on next page)

(Table A-1, Continued)	
28	Misc. Leakage in Secondary System
29	Sudden Opening of Steam Relief Valves
30	Loss of Circulating Water
31	Loss of Component Cooling
32	Loss of Service Water Systems
33	Turbine Trip, Throttle Valve Closure, EHC Problems
34	Generator Trip or Generator Caused Faults
35	Total Loss of Offsite Power
36	Pressurizer Spray Failure
37	Loss of Power to Necessary Plant Systems
38	Spurious Trips - Cause Unknown
39	Auto Trip - No Transient Condition
40	Manual Trip - No Transient Condition
41	Fire Within Plant

TABLE A-2

RISK-CRITICAL COMPONENTS IDENTIFIED BY NON-PRA APPROACH

HARDWARE BY COMPONENT TYPE AND SYSTEM/FUNCTION

COMPONENT TYPE	SYSTEM/FUNCTION	No.
Pumps (All Types) (20)	Auxiliary Feedwater	4
	Feedwater/Condensate	4
	Low Pressure Injection/Shutdown Cooling	2
	High Pressure Injection	2
	Containment Spray	2
	Component Cooling Water	2
	Chilled Water	2
	Service Water	2
Motor-operated Valves (47)	Auxiliary Feedwater	9
	Feedwater/Condensate	2
	Low Pressure Injection/Shutdown Cooling	10
	High Pressure Injection	12
	Containment Spray	8
	Safety Injection (General)	4
	Component Cooling Water	2
Solenoid Valves (21)	Safety Injection	10
	Reactor Coolant (Venting)	7
	Main Steam	4
Relief Valves	Main Steam	27
Main Steam Isolation Valves(MSIV)	Main Steam	4
Atmospheric Dump Valves (ADV)	Main Steam	4

(continued on next page)

(Table A-2, Continued)		
Primary Safety Valves	Reactor Coolant	4
Check Valves (All Types) (51)	Auxiliary Feedwater	9
	Feedwater/Condensate	2
	Low Pressure Injection/Shutdown Cooling	4
	High Pressure Injection	8
	Containment Spray	4
	Safety Injection	16
	Service Water	2
	Main Steam	6
Chiller Units	Chilled Water	2
Air Cooling Units	HVAC	10
Strainers	Feedwater/Condensate	2
Pressure Transmitters (All Types) (40)	Emergency Safeguards Features Actuation System	4
	Emergency Safeguards Features Actuation System/Reactor Protection System	8
	Reactor Protection System	28
Level Transmitters (12)	Emergency Safeguards Features Actuation System	4
	Emergency Safeguards Features Actuation System/Reactor Protection System	8
Temperature Elements	Reactor Protection System	12
Neutron Flux	Reactor Protection System	4
Control Element Assembly Position	Reactor Protection System	89
CEA Calculators	Reactor Protection System	89

(continued on next page)

(Table A-2, Continued)		
Bistables (157)	Emergency Safeguards Features Actuation System	24
	Reactor Protection System	133
Initiation Logic (12)	Emergency Safeguards Features Actuation System	6
	Reactor Protection System	6
Initiation Circuits	Reactor Protection System	4
Actuation Logic (14)	Emergency Safeguards Features Actuation System	12
	Reactor Protection System	2
Trip Breakers	Reactor Protection System	4
	Total:	629

TABLE A-3

CANDIDATE RISK-CRITICAL PASSIVE COMPONENTS IDENTIFIED BY NON-PRA APPROACH

HARDWARE BY COMPONENT TYPE AND SYSTEM/FUNCTION

COMPONENT TYPE	SYSTEM/FUNCTION	No.
Heat Exchangers (4)	Low Pressure Injection/Shutdown Cooling	2
	Component Cooling Water	2
Steam Generators	Main Steam	2
Reactor Vessel	Reactor Coolant	1
Accumulators	Main Steam	4
Tanks	Chemical Volume Control (RWST)	1
	Total:	12

TABLE A-4

RISK-CRITICAL ELECTRICAL COMPONENTS IDENTIFIED BY NON-PRA APPROACH

COMPONENT AND NUMBER OF COMPONENTS	
Main Switchyard	1
Transformers (12):	
Main	3
Auxiliary	1
Emergency Safeguards Features	2
Load Center	6
Buses (20):	
Intermediate	2
High Voltage Emergency Safeguards Features	2
4.16 KV	2
480 V	6
Motor Control Center	8
Circuit Breakers (40):	
Emergency Safeguards Features Bus	2
High Voltage	2
Emergency Safeguards Features Main	2
4.16 KV Supply	6
480 V Main Feeder	6
Motor Control Center Feeder	8
Battery	4
Battery Charger	4
DC Panel Feeder	4
Diesel Generator	2
Diesel Generators	2
Batteries	4

(continued on next page)

(Table A-4, Continued)	
Battery Chargers	4
DC Control Center	4
DC Distribution Panel	4
Total:	91

TABLE A-5

RISK-CRITICAL COMPONENTS IDENTIFIED BY NON-PRA APPROACH

BY SYSTEM

SYSTEM AND NUMBER OF COMPONENTS	
Auxiliary Feedwater	22
Component Cooling Water	6
Chilled Water	4
Service Water	4
Chemical Volume Control	1
Feedwater/Condensate	10
Main Steam	51
Reactor Coolant System	12
HVAC	10
Emergency Core Cooling System (88 Components)	
General/Common	34
Low Pressure Injection/Shutdown Cooling	18
High Pressure Injection	22
Core Spray	14
Emergency Safeguards Features Actuation System (ESFAS)	62
Reactor Protection System	371
Electric Power	91
Total:	732

TABLE A-6

SUMMARY OF TRANSIENTS IDENTIFIED IN NON-PRA APPROACH

(FOUR YEARS OF LERs REVIEWED FOR A PWR)

TRANSIENT	CATEGORY (s)	No. of Events
Feedwater Flow Problems	15,21,22	15
Loss of Power to Plant Systems	35,37	10
CRDM Problems	3,3a	9
Generator Trip	34	6
Loss of RCS Flow/Reduced RCS Flow	1,14,14a	5
Turbine Trip/Turbine Faults	33	3
High/Low Pressurizer Pressure	6,8	3
Primary System Leakage	5	1
Sudden Opening of Relief Valves	29	1
Auto Trip - No Transient Condition	39	1
Manual Trip - No Transient Condition	40	1
	Total:	55

APPENDIX B

DEMONSTRATION OF PRA APPROACH FOR DETERMINING RISK-CRITICAL COMPONENTS

B.1 INTRODUCTION

A completed, Level I probabilistic risk assessment (PRA) for a BWR plant was used for this demonstration of the determination of risk-critical components when a PRA is available. The demonstration included:

- the determination of risk-critical components from the accident sequences represented in the PRA,
- the determination of important initiators of accidents from the PRA, and
- the determination of risk-critical components for the "Loss of Feedwater" initiator for the BWR plant.

The determination of risk-critical components for other initiators is expected to involve similar steps as those performed in this demonstration. Also, risk-critical passive components were not determined in this demonstration; a plant which uses their PRA would use the same methodology for passive components as that illustrated in Appendix A, "Demonstration Of Approach For Identifying Risk-Critical Components When A PRA Is Not Used".

B.2 APPROACH DESCRIPTION -- DEMONSTRATION-SPECIFIC

Although the PRA approach for determining risk-critical components is generally simple and straightforward, the specific steps or tasks which must be performed will vary depending upon the structure and modeling style used to perform the PRA. Sections B.2.1 and B.2.2 describe those steps taken to identify risk-critical components from accident sequences and for the "Loss of Feedwater" initiator, respectively. However, the first two steps of these separate demonstrations are identical and are discussed in the paragraph below.

The first task of the PRA approach is the selection of an appropriate fraction of the core melt frequency upon which to base the definition of risk-critical. For this demonstration, an agreement was reached between SAIC and the cooperating utility to use, as a maximum, 90.9 % of the total core melt frequency as the base definition of "risk-significance." The second necessary step is to identify and rank all the accident sequences (including initiating event frequencies) that comprise the chosen fraction according to their contributions to 90.9% of the core melt

frequency. In this demonstration, the PRA results provided by the cooperating utility satisfied this information requirement.

B.2.1 Risk-Critical Component Determination from Accident Sequences

Like most PRAs, the PRA used for this demonstration was modularized (i.e., several failure modes for different components, which make equivalent contributions logically, are grouped). As a result, tracing back from the PRA results (i.e., accident sequences) to component failure modes required the use of the PRA's accident sequences, module definitions, and basic event listings in order to identify unique, risk-critical components. Three major steps were involved in this identification of (primarily standby and operating) risk-critical components: 1) the determination of accident sequence composition, 2) the identification of risk-critical components by the appearance of their failure modes in the ultimate compositions of the accident sequences, and 3) the verification, and possible modification, of the resulting list of risk-critical components through the use of the PRA's modeling assumptions. Each of these three steps, as well as advantages and disadvantages of using a modularized PRA, are discussed below.

In turn, the determination of the composition (i.e., which modules or top-events) of the accident sequences contributing to 90.9% of the core melt frequency involved several steps. Using the ranked accident sequences provided by the cooperating utility, a unique set of events (e.g., modules, top-events, basic events, etc.) contributing to 90.9% of core melt frequency was determined. The ranked accident sequences were then further partitioned according to their core melt frequency contributions (i.e., ~ 50%, 75%, and 90% of the total core melt frequency). In this demonstration, a unique module or top-event was identified by assigning the event to the highest ranking accident sequence of which it was a contributor, then eliminating it as a contributor from all other accident sequences. Unique basic events (e.g., component failure modes) were identified similarly. Using the number of unique contributors in each partition of core melt frequency as the basis, the appropriateness of the core melt frequency fraction selected was then assessed.

The final task for identifying risk-critical components from accident sequences involves the use of the PRA's module definitions and basic event listing (i.e., master data file). The basic event file verifies if a unique event identified in the steps above is a module or a basic event. The composition of the identified unique modules is determined using the module definitions (i.e., listings of events comprising the module). Then, the basic events identified from the module definitions, as well as the basic events already identified, can be matched up with the failure descriptions given in the basic event file. For the purposes of determining risk-critical components, only basic events which are component

failure modes are of interest. Hence, the following types of basic events are eliminated from consideration:

- human errors,
- initiators,
- module names,
- test and maintenance unavailabilities, and
- common cause failures (CCFs) which represent multiple failure modes. (However, if a CCF is the only failure mode for a group or single component, those components should be added to the risk-critical component list.)

In order to compile the list of risk-critical components, once a risk-critical component was identified from the matchup of a basic event and description of its failure mode, subsequently identified failure modes for the same risk-critical component (i.e., multiple failure modes) were ignored in this demonstration. In addition, the lack of notation in the basic event file descriptions of the PRA used for this demonstration resulted in the inability to match up some electrical components (e.g., relays, contact pairs, fuses, etc.) with their associated, risk-critical equipment (e.g., pumps, MOVS, etc.). This complication could be solved by consultation with the PRA staff at the cooperating utility. However, the risk-criticality of these components could also be verified in the risk-focused maintenance (RFM) process. The RFM process could also make use of risk-critical lists composed of the common cause failures, human errors, and component-specific multiple failure modes which were discarded in this demonstration.

A final check of the resulting risk-critical component list should be made, recognizing that these results are based upon various PRA modeling assumptions which are usually documented in the PRA study report. For instance, in this demonstration, components which were in parallel equipment trains and served the same function as an identified risk-critical component were added to the risk-critical component list. These components are expected to have been excluded from the results due to such modeling assumptions as "Train A normally operating," "LOCA on injection leg #1," etc. In addition, the risk-critical component list should be reviewed in order to verify that support equipment for identified risk-critical components has been included. For instance, in this demonstration, the PRA staff of the cooperating utility could verify the appropriate inclusion of containment cooling, HVAC support, and any associated chilled water requirements.

Modularization of PRAs is a useful, time-saving strategy. However, for the purpose of identifying risk-critical components, modularized PRAs are not completely ideal tools. Because several

components, in the form of their failure modes, appear together in a module, some very reliable components (e.g., relays, open manual valves, etc.) may be identified as being risk-critical because of their association with one or more less reliable, safety important components. Hence, more components are identified as risk-critical than would be if the PRA was not modularized. However, usually, these modules represent logical groupings of components which can either reduce the redundancy or fail a system function. Hence, the components and their failure modes in these modules can be useful in the RFM process as super-component "failure modes."

B.2.2 Risk-Critical Component Determination from Initiating Events

The purpose of this demonstration is to illustrate how to identify risk-critical components, primarily in normally operating systems and balance-of-plant (BOP) systems, from initiating events. There are only two main steps to this identification of risk-critical components: 1) the determination of a list of risk-critical initiators and 2) the identification of components which are the likely causes or drivers of each risk-critical initiator. The second step is common to both the PRA and non-PRA approaches for risk-critical component determination. Both steps are further discussed below.

In the PRA approach, the list of risk-critical initiators is developed from the ranked accident sequences, such as that provided by the cooperating utility for 90.9% of the total core melt frequency. In this demonstration, the initiators represented in the PRA results were also ranked based upon the contributions either from the individual accident sequences associated with each unique initiator or from the sum of all associated sequence contributions for each unique initiator. From this preliminary list of initiators, initiators for which there is no prevention (e.g., external events) should be eliminated.

Regardless of approach (i.e., PRA or non-PRA), there are various information sources useful for the identification of candidate risk-critical components once the risk-critical initiator list is developed. For this demonstration involving the "Loss of Feedwater" initiator, a combination of plant-specific and generic data sources were used. Licensee Event Reports (LERs), plant incident reports, and corrective maintenance records pertinent to the Feedwater System for the cooperating plant were consulted. Reference B-1, "Analysis Of Reactor Trips Originating In Balance Of Plant Systems", was used due to the fact that it contains generic component drivers for BOP initiators. Any input used in deriving the initiating event frequency may be useful to the identification of associated risk-critical components. For instance, if system fault trees were developed for the purpose of providing an initiator frequency, they could be solved and component importance

rankings found in order to identify the most important drivers of a system initiating event (e.g., "Loss of Service Water").

B.3 RESULTS OF APPLYING PRA APPROACH FOR DETERMINING RISK-CRITICAL COMPONENTS

The results of applying the PRA approach to a BWR plant are shown in three sets of tables. These tables correspond to, respectively, the generic PRA-approach task of selecting an appropriate fraction of the core melt frequency for the definition of risk-critical and to the tasks of identifying risk-critical components from accident sequences and from initiating events. These tables, and their accompanying discussions, are given below.

The results of the assessment task described in Section B.2.1 are shown in Table B-1. Based upon the number of contributors, unique modules and basic events, to the three partitions of 90.9% of the core melt frequency, it appears that using a core melt frequency fraction which is smaller than 90.9% for the basis of risk-criticality is justified for the PRA used in this demonstration. Another way to potentially justify the use of a fraction less than 90.9% could involve the number of times each module is involved in an accident sequence, both overall and by partitions of the core melt frequency. Despite the results of Table B-1, 90.9% of core melt frequency, as agreed upon by the cooperating utility, was used for determining risk-critical components in this demonstration.

TABLE B-1

COMPARISON OF NUMBER OF CONTRIBUTORS TO PARTITIONED CORE MELT FREQUENCY

Number of Contributors	Percentage of Core Melt Frequency *		
	0-50%	50-75%	75-90%
Unique Modules	34	16	22
Basic Events	552	163	68

Table B-2 shows the risk-critical components, which were identified as described in Section B.2.1, by component type for all plant systems except electric power. Components identified which are part of the electric power system, shown in Table B-3, have been divided into three groups. The first group consists of major risk-critical components (i.e., diesel generators, buses, MCCs, etc.).

---

* Percentages are approximate.

TABLE B-2

RISK-CRITICAL ACTIVE COMPONENTS IDENTIFIED BY PRA ACCIDENT SEQUENCES

COMPONENT TYPE	SYSTEM/FUNCTION	No.
Pumps (All Types) (33)	Core Spray	2
	Feedwater/Condensate	10
	Low Pressure Injection	4
	Main Steam	1
	Standby Liquid Poison	2
	Service Water	4
	Other Cooling Water System	8
	Firewater	2
Motor-operated Valves (17)	Feedwater/Condensate	1
	Isolation Condenser	2
	Low Pressure Injection	6
	Main Steam	2
	Service Water	1
	Other Cooling Water Systems	3
	Reactor Water Cleanup	2
Air-Operated Valves	Reactor Water Cleanup	1
Check Valves (All Types) (38)	Core Spray	4
	Feedwater/Condensate	10
	Isolation Condenser	2
	Low Pressure Injection	8
	Standby Liquid Poison	6
	Service Water	4

(Continued on next page)

(Table B-2, Continued)		
(Check Valves, Cont.)	Other Cooling Water Systems	4
Relief Valves (7)	Automatic Depressurization	6
	Reactor Water Cleanup	1
Safety Relief Valves		30
Manual Valves (9)	Core Spray	2
	Service Water	5
	Other Cooling Water Systems	2
Strainers	Other Cooling Water Systems	2
Vent Header	Reactor Coolant (Venting)	1
Vent Line	Reactor Coolant (Venting)	1
Downcomer Pipe	Reactor Coolant (Venting)	1
Vacuum Breaker	Reactor Coolant (Venting)	1
High Drywell Pressure Sensor	Emergency Safeguards Feature Actuation System/Low Pressure Injection and Core Spray	4
Low-Low Reactor Level Sensor	Emergency Safeguards Feature Actuation System/Low Pressure Injection and Core Spray	4
Switches, Pressure (15)	Feedwater/Condensate	14
	Reactor Water Cleanup	1
Switches, Level (3)	Feedwater/Condensate	2
	Isolate Condenser	1
Switches, Manual	Other Cooling Water Systems	1
Switches, Common Start	Standby Liquid Poison	1
	Total:	169

TABLE B-3

RISK-CRITICAL ELECTRICAL COMPONENTS IDENTIFIED BY PRA

BY COMPONENT TYPE

COMPONENT TYPE AND NUMBER OF COMPONENTS	
Main Switchyard	1
Emergency Gas/Turbine Generator	1
Emergency Diesel Generator	1
Diesel Generators	2
Motor Generator Set	1
Buses (11):	
High Voltage - AC	7
Medium Voltage - AC	2
Low Voltage - AC	1
Vital AC	1
DC Batteries	2
Transformers	4
Motor Control Centers (5):	
400 V	4
DC	1
DC Switchboards	4
DC Panels	5
Automatic Bus Transfer	2
Circuit Breakers (All Types)	91
Coils (All Types)	69
Contact Pairs	230
Auxiliary Breaker Contacts	2
Relays (All Types)	30
Fuses	15
Control Switches	3
Total:	479

The second group, which is wholly comprised of circuit breakers, is separated from other electric power components. The reason for this separation is that, while the PRA results indicate that these circuit breakers are risk-critical components, the lack of adequate description in the basic event file regarding the function of the majority of the breakers made it difficult to assess their relative importance or to put their importance in the correct context. For instance, it would be useful to know if a breaker is associated with a motor control center (MCC), which serves many electrically-powered components, or if it is associated with only one electrically-powered component (e.g., pump, MOV). Like the circuit breakers, the components in group #3 cannot all be associated with their companion electrically-powered component due to the lack of description in the basic event file. As noted in Section B.2.1, the risk-criticality of these components could be verified as part of the reliability-focused maintenance (RFM) portion of this overall approach. For instance, in the RFM portion of the maintenance program for a risk-critical component, all reasons for pump failure, including failure of circuit breakers, relays, lube oil cooling water delivery, etc., could be considered. Another reason for grouping these components separately is that, since electrical components, in general, are more reliable than mechanical equipment, they are likely to have been included in the PRA results only by their association with less reliable, safety-important components. It is possible, and can be verified as part of the RFM process, that these generally highly reliable electrical components are not one of the important "failure modes" (e.g., pump fails to start, breaker fails to close, relay fails to transfer, component cooling water valve fails to open, room cooler fails to start, etc.) of a risk-critical component.

Table B-4 summarizes the total number of risk-critical components identified from the accident sequences by system. Note that without any electrical components, there are approximately 200 risk-critical components identified. With major electrical components and circuit breakers included, there are about 300 risk-critical components. The remaining electrical components should be regarded as candidate risk-critical components which should be verified either as part of the reliability-focused maintenance process or in a PRA/RCM interfacing task.

Table B-5 shows the initiators associated with the 90.9% of the core melt frequency for this PRA. The table shows both the rank of the initiator, as determined by the most dominant of its associated accident sequences, and the cumulative contribution of all its associated accident sequences. For the "Loss of Feedwater" initiator, shown in Table B-5 to be one of the most important initiators, the associated risk-critical components were determined.

TABLE B-4

RISK-CRITICAL COMPONENTS IDENTIFIED BY PRA

BY SYSTEM

SYSTEM AND NUMBER OF COMPONENTS	
Core Spray	8
Feedwater/Condensate	37
Isolation Condenser	5
Low Pressure Injection	18
Main Steam	3
Standby Liquid Poison	9
Service Water	14
Other Cooling Water Systems	20
Fire Water	2
Emergency Safeguards Feature Actuation System	8
Relief Valves	36
Reactor Coolant	4
Electric Power *	39
Reactor Water Cleanup	5
SubTotal:	208
Electric Power **	91
SubTotal:	299
Electric Power ***	349
Total:	648

* Includes major equipment such as the switchyard, diesel generators, buses, MCCs, batteries, transformers, switchboards, panels, etc.

** Breakers only.

*** Includes coils, contact pairs, relays, fuses, breaker contacts, and control switches.

TABLE B-5

CRITICAL INITIATORS IDENTIFIED BY PRA FOR A BWR PLANT

INITIATOR *	HIGHEST RANK IN SEQUENCES	PERCENT CONTRIBUTION TO CORE MELT FREQUENCY OF ASSOCIATED SEQUENCES **
Loss of AC Power	1	13.7
Loss of Feedwater	2	11.0
Small Break LOCA	3	11.4
Loss of Offsite Power	4	14.8
Small Small Break LOCA	5	5.1
Large Break LOCA	6	2.9
Reactor Transient w/Main Condenser Available	7	9.8
Inadvertent Opening of Safety Relief Valves	8	2.7
Anticipated Transient Without SCRAM (ATWS)	9	3.6
Loss of Service Water	10	4.6
Reactor Trip	11	6.1
Reactor Transient w/o Main Condenser	12	3.0
V-Sequence	13	0.7
Loss of Other Cooling Water Systems	14	0.6
Total:		90.9 **

* Components which make significant contributions to the initiating frequencies should be identified for all initiators except LOCAs and external initiators.

** Round-off errors in tabulated percentages

This determination was made as described in Section B.2.2 using plant-specific and generic sources of information regarding initiator drivers. The results of this determination, shown in Table B-6, result in the addition of only three risk-critical components: feedwater regulating valves. The other risk-critical components identified in Table B-6 were already identified as part of the accident sequence risk-critical component determination.

B.4 ASSUMPTIONS AND OTHER NOTATIONS

Two notes should be made regarding this approach for risk-critical component determination: 1) the results of this approach are dependent upon modeling assumptions which are not obvious by simply reviewing the PRA results and 2) the interface between this, or any other, approach for risk-critical component determination and the reliability-focused maintenance process is important. Both of these issues are discussed briefly below.

There are typically many assumptions made in a PRA. These assumptions dramatically influence the results obtained for a PRA and, therefore, for the PRA approach for risk-critical component determination. Hence, knowledge and understanding of these assumptions is important in the initial determination of risk-critical components as well for any updates of the risk-critical component list. An exhaustive and generic list of modeling assumptions which are important to the approach described in this appendix is not possible. However, examples of important assumptions regarding component failure rates are: 1) the assumed maintenance environment, as reflected in plant-specific data, does not change, 2) the modeled operating environment (i.e., hours of operation or number of tests, etc.) does not change, and 3) components do not age or degrade (i.e., failure rates are constant). One obvious result of such assumptions is the exclusion of the usually highly reliable Control Rod Drive System.

The interface between the determination of risk-critical components and the reliability-focused maintenance process (which parallels the Reliability-Centered Maintenance (RCM) process) should be considered prior to initiating an overall risk-focused maintenance program. The motivation for such consideration stems from the differences between PRAs and traditional RCM studies with regard to the definition of component "failure modes" and the treatment of system boundaries. For instance, with a PRA, risk-critical components and their critical failure modes (i.e., fails to start, fails to run, fails to open or close, fails to remain open or closed, fails to transfer, etc.) can be identified. However, traditional RCM studies are typically concerned with the underlying causes of component failure modes, as defined in the PRA community. While integrating these two approaches can be potentially useful, since together they progressively focus in upon component failures causes or mechanisms, consideration of how to integrate the two processes should be done up front. Assuming that risk-critical

TABLE B-6

CANDIDATE RISK-CRITICAL COMPONENTS FOR "LOSS OF FEEDWATER" INITIATOR *

COMPONENT TYPE AND NUMBER OF COMPONENTS		
Feedwater Regulating Valve		3
Feedwater Pumps	**	3
Condensate Pumps	**	7

* Based upon plant-specific LERs and Plant Incident Reports and generic information.

** Already identified in accident sequences of PRA.

component determination is performed using a PRA, there are two possible scenarios: 1) traditional RCM programs and studies which are existing or planned will be used, 2) reliability-focused maintenance programs specifically designed for interface with risk-critical component determination will be used. As a result of differing treatments of system boundaries, a key difference exists between these two scenarios regarding in which support system failures are treated. In PRAs, support system failures are treated logically with the component(s) being supported. In traditional RCM studies, this is not the case; RCM studies are performed on a system basis, with fairly strict adherence to system boundaries. A reliability-focused maintenance program could be designed to easily interface with PRAs through the use of the logical coupling of support systems with their supported components. When a traditional RCM program is interfaced with PRA risk-critical component determination, additional work to achieve the interface is required. For instance, a utility may identify either all the electrical components contained in the PRA results (including relays, coils, fuses, etc.) or all electrical components modeled in the PRA as risk-critical components. Or, a utility may elect to identify additional electrical components as risk-critical after reviewing maintenance work records for risk-critical components and their associated supporting components.

B.5 CONCLUSIONS

Overall, the performance of this demonstration went as planned. In reviewing the contributors to the accident sequences for this PRA, it was evident that the majority of the modules and their associated component failure modes, could have been captured by using only 75% of the PRA results. However, risk-critical components for all available PRA results were reported. It is anticipated that application of this PRA approach to other PRAs will involve similar efforts and results. However, since PRAs do differ in the way they are modularized or structured, there may be subtle differences in the actual steps of tracing back from the PRA results to the associated components, and their failure modes.

REFERENCES

B-1. Stetson, F. T.; Gallagher, D. W.; Le, P. T.; and Ebert, M. W.; "Analysis of Reactor Trips Originating in Balance of Plant Systems", prepared for U.S. NRC, SAIC-89/1148, September 1989.

APPENDIX C

DEMONSTRATION OF RELIABILITY-FOCUSED MAINTENANCE FOR STANDBY COMPONENTS

C.1 INTRODUCTION

This appendix contains the reliability-focused maintenance (RFM) demonstration for components in a standby system. For the purposes of this demonstration, an existing Reliability-Centered Maintenance (RCM) study, which was completed approximately a year prior to the start of the Risk-Focused Maintenance project, was used. The risk-critical components of the Auxiliary Feedwater (AF) System identified in the Non-PRA approach applied given in Appendix A are highlighted in this demonstration.

C.1.1 Motivation for Using RCM Study in Demonstration

There were a variety of reasons for using an existing, utility-sponsored RCM study for the demonstration of the reliability-focused maintenance process. Most importantly, the results obtained in this RCM study for the identified risk-critical components of the AF system are regarded as acceptable for the reliability-focused maintenance process. Since the performance of this RCM study was consistent with the EPRI RCM methodology (Reference C-1), it is expected that the results of similar utility or industry-sponsored studies for standby safety systems would be similarly acceptable. (See Appendix D, "Demonstration Of Reliability-Focused Maintenance For A Normally Operating System", for discussion regarding normally operating systems.) In addition, potential confusion between the RCM and RFM methodologies can be addressed through direct comparison, which is given in the following section.

C.1.2 Differences and Similarities Between RCM and RFM Methodologies

The really crucial difference between the reliability-centered maintenance (RCM) and reliability-focused maintenance (RFM) processes relates to the purposes of the two processes. As part of Risk-Focused Maintenance, the purpose of reliability-focused maintenance is to optimize maintenance from a safety standpoint, for already identified risk-critical components (identified through either the PRA or non-PRA approaches). The goal of reliability-centered maintenance is to optimize maintenance from both safety and economic (e.g., optimization of the balance between time-directed vs. condition-directed tasks) standpoints. In addition, part of the RCM methodology involves a determination of component "criticality". This determination of "criticality", which includes consideration of component reliability, unavailability, and system function and design, differs from the approaches demonstrated in

Appendices A and B in that it does not include consideration of the relative importance of components on a plant-wide basis with respect to required accident response, to initiating accidents, or to essential support of front-line safety systems. As illustrated in Appendix D, the difference between risk-critical and RCM "criticality" is more pronounced for a normally-operating system.

In comparing the major tasks performed in the AF RCM study with Figure 5-3, "Summary Of Process For Determining Dominant Failure Modes Of Risk-Critical Components", which outlines the reliability-focused maintenance process, there appears to be considerable similarity between the two approaches. Path C in Figure 5-3 is identical to the tasks discussed in Sections C.2.4 and C.2.5. A qualitative analysis, rather than the quantitative analysis indicated in Path B of Figure 5-3, was performed as part of the task discussed in Section C.2.3. However, either quantitative or qualitative failure history analysis may be appropriate and, in some cases, sparse data may preclude the performance of quantitative analysis. From Figure 5-3, the Path A tasks of the reliability-focused maintenance process appear to coincide with the fault tree analysis and FMEA tasks of the RCM study. However, the fault tree analysis of the RCM study is performed on a system basis, rather than for risk-critical components to the piecepart level. The purpose of this system-level fault tree, which is similar in some ways to that which could be used in a PRA, is to calculate component importance rankings, which are used along with Figure C-1 to establish component "criticality" in the RCM process. Hence, a system-level fault tree, such as that performed in the AF RCM study, would not be performed as part of the RFM process since it is redundant to the risk-critical component determination approaches illustrated in Appendices A and B. In addition, the FMEA task, as performed in the AF RCM study, also does not go to the piecepart or failure mechanism level (sometimes called "failure mode" within the RCM community); the lowest level of detail in the RCM study is the component failure mode, as defined in the PRA community and used throughout this report (i.e., component fails to start or run, component fails to open or close). However, the performance of FMEA to the piecepart level may be important only in the identification of failure drivers for risk-critical components which have a high corrective maintenance (CM) load relative to preventive maintenance.

Another, less important, difference between the RCM and RFM processes relates to the definition of component and system boundaries for the purposes of investigation. For the purposes of the reliability-focused maintenance process, it may be useful to define system and component boundaries solely upon the basis of the functions served in accident response (or initiator cause). Such definitions of system and component boundaries, which are consistent with PRA methodology regarding fault tree modeling and module determination with fault trees, are not usually consistent

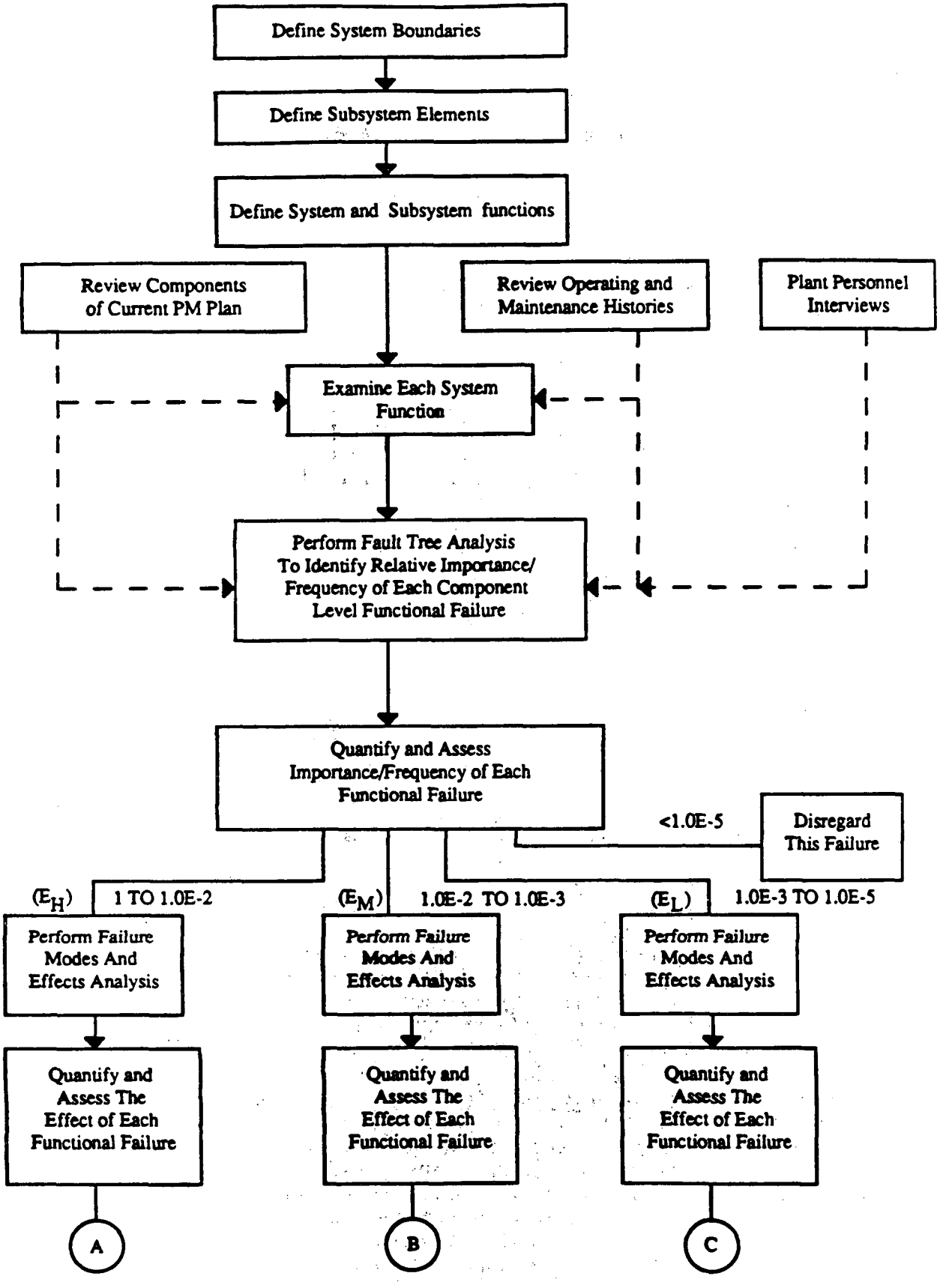


Figure C-1. RCM Methodology Process Diagram

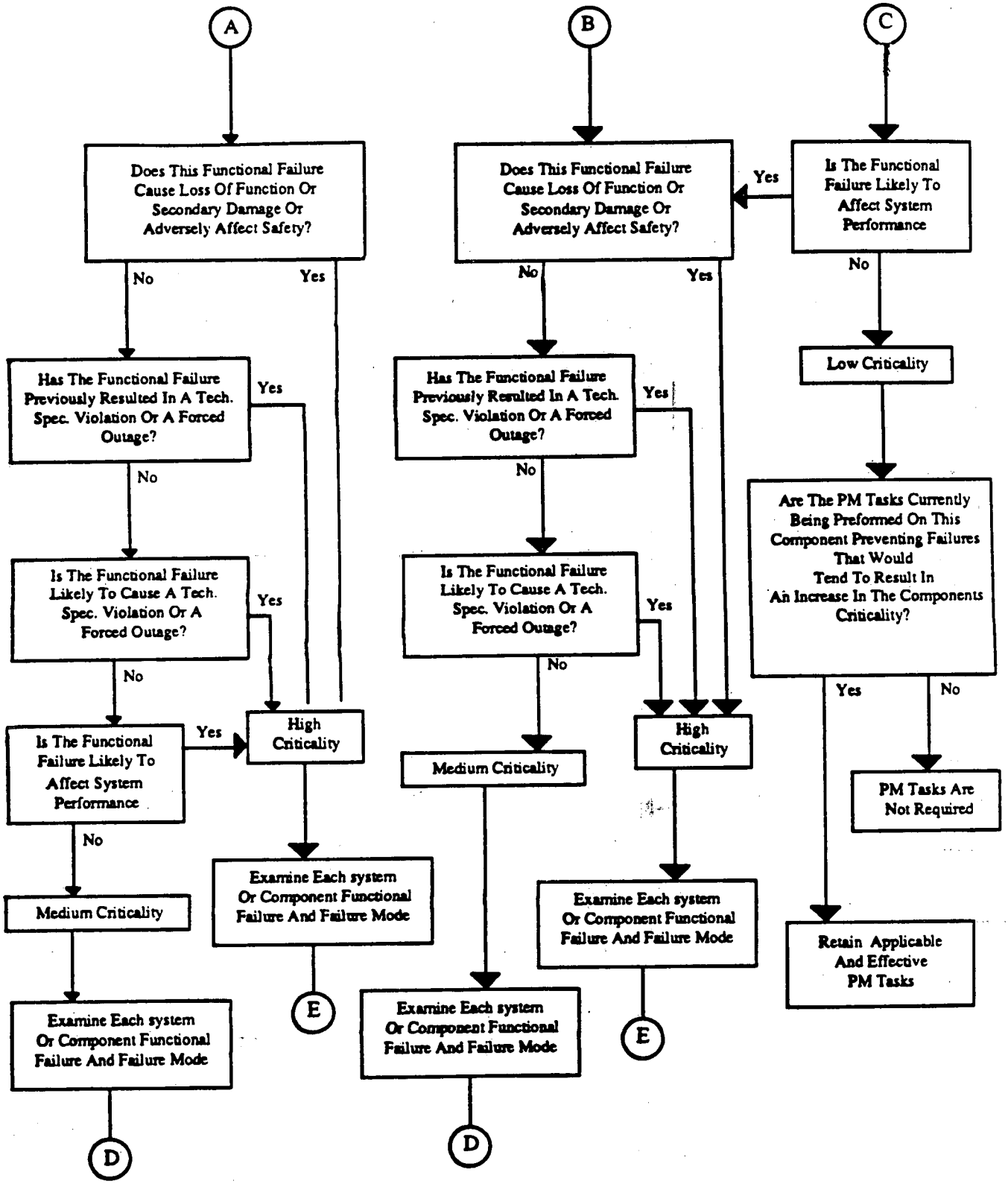


Figure C-1. RCM Methodology Process Diagram (Continued)

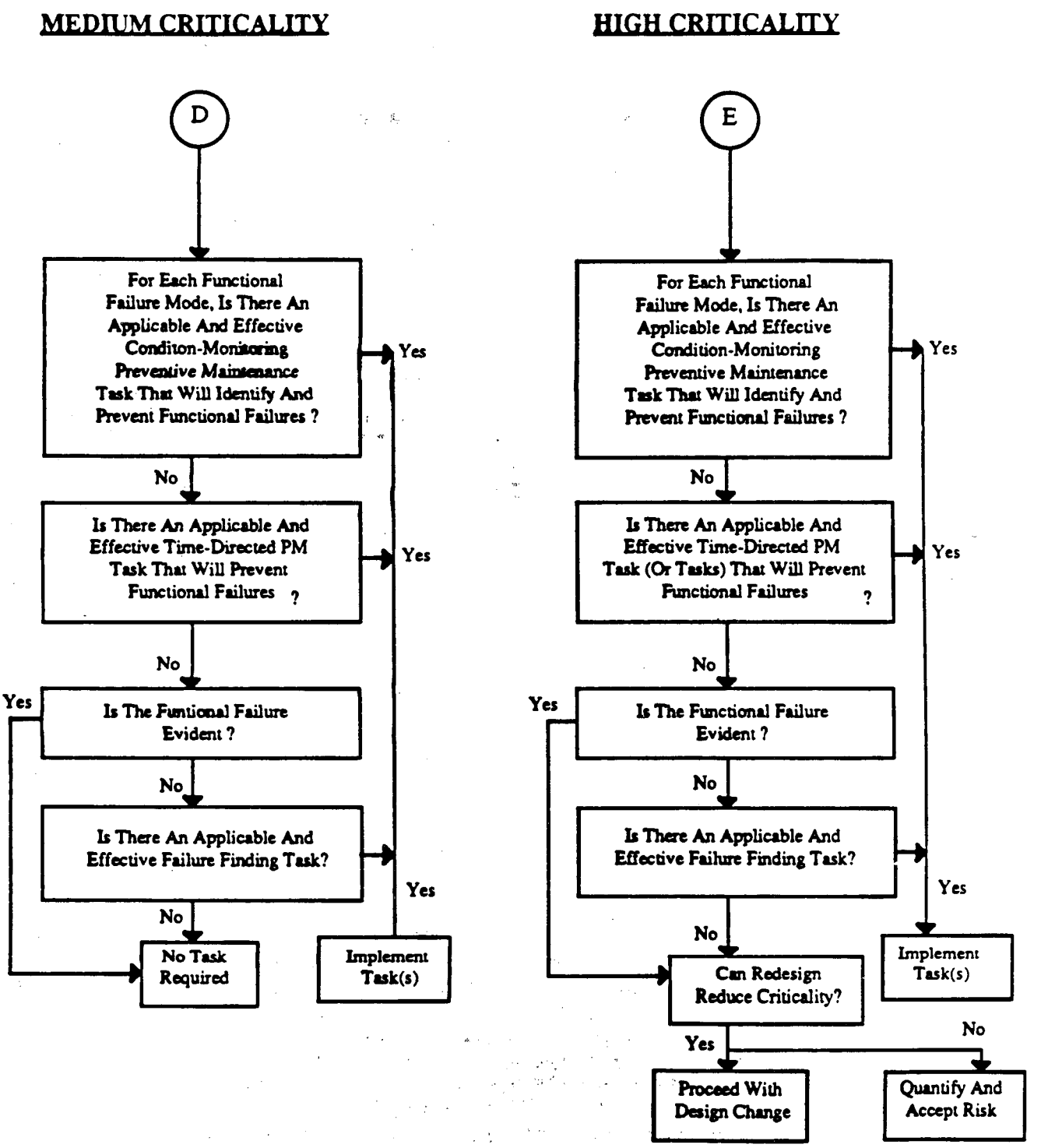


Figure C-1. RCM Methodology Process Diagram (Continued)

with traditional RCM studies or with the specific RCM study being used in the appendix. In traditional RCM studies, system and component boundaries may be defined by the nomenclature used in system drawings (e.g., any component labeled with the "AF" prefix is part of the auxiliary feedwater system and anything else is not). (If the maintenance work record system uses the same system boundaries, gathering information on corrective maintenance history can be aided by this RCM-based definition of system boundary.)

There are two main advantages to the PRA-based boundary definitions. First, because there are typically many interconnections and shared components between systems in nuclear power plants, a function-based approach to system boundary definition provides a logical basis for minimizing the possibility of "missing" components. By using the traditional RCM-based definition of system boundary, the utility is committed to performing several RCM studies in order to avoid missing the identification of important components in other systems. (For instance, the demonstration in Appendix A, "Demonstration Of Approach For Identifying Risk-Critical Components When A PRA Is Not Used", for the AF system included the identification of six check valves in the Main Steam system which were required for AF system accident response. However, these check valves were not also identified as being risk-critical to the function of the Main Steam system in responding to an accident. As a consequence of the traditional RCM system boundary definition, these check valves, which are important to the success of AF system response to an accident, are not included in the AF RCM study and their importance may not be recognized in a hypothetical Main Steam RCM study.) Secondly, an expanded component boundary may be useful as part of an RCM or RFM process in identifying the failure drivers for a risk-critical component which is determined to have a relatively high CM load (see discussion of FMEA above). This potential advantage is based upon the observation that, in maintenance records, degradations or failures are frequently assigned to the major component which is directly impacted and for which discovery is more likely through periodic testing or surveillance. For instance, the failure of a circuit breaker, considered part of the electric power system in the traditional RCM-based definition, may be assigned to the motor-operated valve it supports. Also, as indicated in the PRA approach of risk-critical component demonstration of Appendix B, the importance of electrical components (e.g., relays, contact pairs, etc.) could be verified through the use of extended component boundaries when performing a failure modes and effect analysis (FMEA) or a component or module-level fault tree analysis solved to the piecepart level.

C.1.3 Appendix Contents

The following sections are primarily excerpts from the RCM study performed for the PWR plant of the cooperating utility approximately a year ago. This appendix focuses upon the results

of the RCM study rather than upon complete documentation of the original study. Where applicable, comparisons and contrasts are made between the RCM study results obtained for the AF system as a whole and those for the identified risk-critical components.

C.2 SYSTEM BOUNDARY DEFINITION AND PARTITION

The system boundaries were defined for the AF system in the RCM analysis and the inputs to and outputs from other interfacing systems were also identified. System boundary definition is particularly important when RCM analysis is intended for eventual application on a plant-wide basis or when RCM analysis may be performed on interfacing systems. Strict boundary control and definition avoids analysis overlaps and gaps. The system boundaries for the AF system are defined as follows:

- The load side of switchgear for the AF system power-operated equipment.
- The AF system side of signals generated by other systems based on the status of those systems, including AF system component control circuits.
- The AF system side, as indicated in system drawings, of piping and valves which connect the AF system with the Main Steam, Secondary Chemical Control, Condensate Storage and Transfer, Chemical and Volume Control, and Auxiliary Steam Systems.

Once the system boundaries were identified, each system was partitioned into tiers of functional systems and subsystems. The formation of functional systems and subsystems, which are linked by inputs and outputs, facilitates the grouping of both hardware and function within the system. Figure C-2 shows this system and subsystem partitioning of components and functions.

The AF system was partitioned into subsystems based upon function, unique and vital for the operation of the system as a whole. Each subsystem is therefore, by definition, functionally significant. Each component within a system was also evaluated to identify its functional significance. A System Work Breakdown Structure (SWBS) numbering system was then assigned to define functionally-significant subsystems and components. The SWBS numbering assignment for the AF system is:

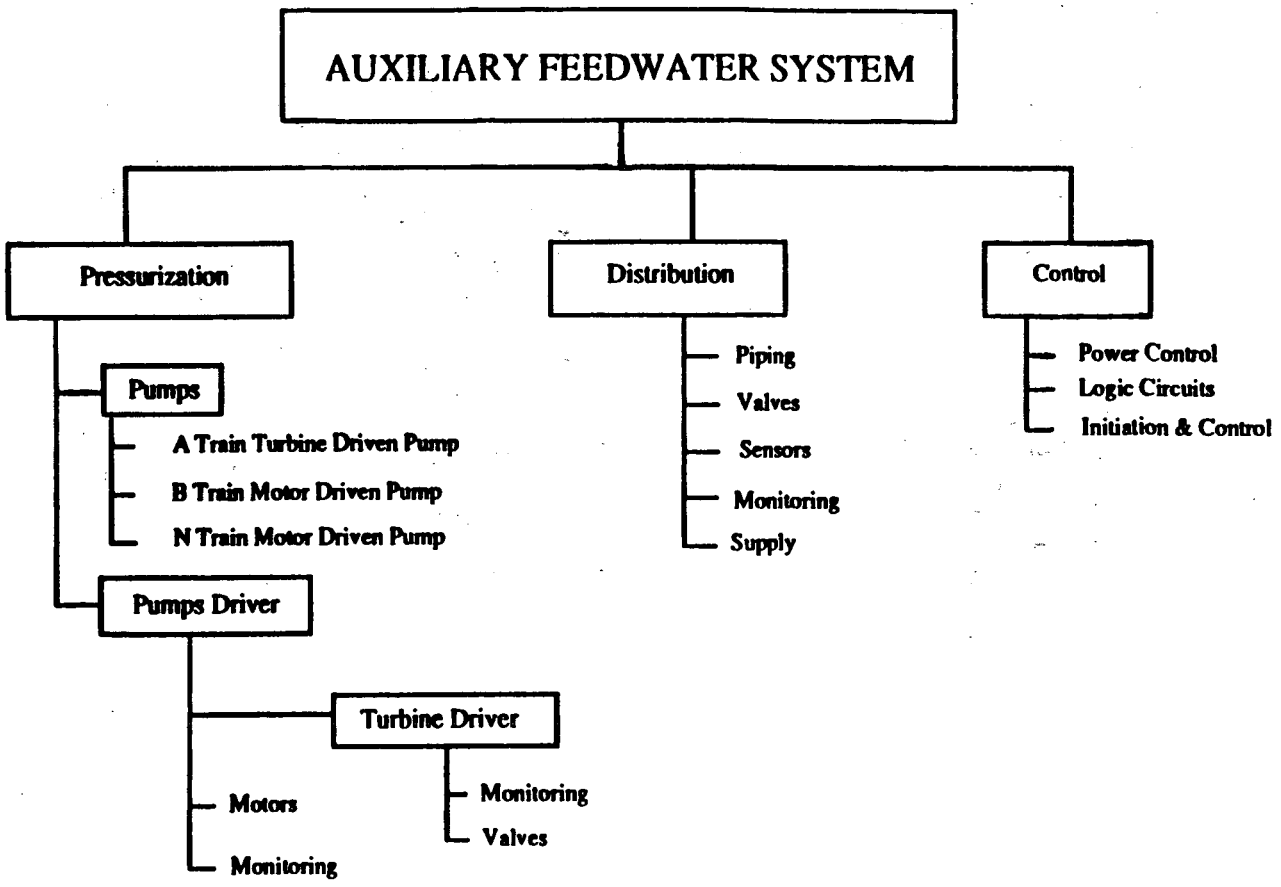


Figure C-2. Functional Block Diagram - Auxiliary Feedwater System

300 Auxiliary Feedwater (AF) System

310 Pressurization
311 Pumps
312 Pump Driver
312.1 Turbine Driver

320 Distribution

330 Control

C.3 FAULT TREE ANALYSIS

For each of the functional partitions identified with a SWBS number, all functions and in or out interfaces were defined. This was done by using Functional Description Forms. An example Functional Description Form for the AF system (SWBS 320: Distribution) is shown in Table C-1. This system-level analysis and definition provided the foundation and framework for conducting a Fault Tree Analysis, whereby the failure modes for each defined function were identified, evaluated, and ranked in terms of importance.

The Fault Tree Analysis provides a logical display of how component failures relate to cause a failure of function. The probability of failure of function was determined by using this logical display, i.e., the fault tree model, quantified with available failure rate data, mission time, and test intervals for each component. Failure rate data was taken from IEEE STD 500 - 1984, "Reliability Data", and other sources, and supplemented by plant-specific information when available.

Most failure rate data available to the nuclear industry (including that used in this report) is based upon the demand scenarios developed in a PRA model. This failure data is not altogether appropriate for use in an RCM analysis where components may run continuously, or near-continuously, from refueling outage to refueling outage, or where a component is started and stopped daily. Therefore, the failure rate data used in the RCM analysis of the AF system was modified if the result of failure rate multiplied by mission time clearly fell outside the bounds of realism. As plant-specific failure rate data continues to be developed over time, the fault tree model can be updated and modified as appropriate.

Each component's mission time, test interval, and demand cycle were based on plant-specific system operating requirements through a period of 365 days. The system operating requirements that were used in this analysis can be found in Table C-2.

The mission times for other components within each system were based on that component's exposure to system operation, which is a function of the component's relationship to the equipment in Table

Table C-1

EXAMPLE FUNCTIONAL DESCRIPTION FORM

SWBS 320 Distribution
Functions and Out Interfaces:
1. Provide the means to add hydrazine from the Secondary Chemical (SC) system through AF Pump #1 to either or both of the SG system steam generators.
2. Provide the means to add ammonia from the SC system through AF Pump #3 to either of both of the SG system steam generators.
3. Provide the means to supply water from the CT system or the CH system to either or both of the SG system steam generators.
4. Provide independent circulation of the discharge of AF Pumps #1, #2, and #3 to the CT system.
5. Provide isolation of the discharge of AF Pumps #1 and #2 to the SG system with HV-30, UV-35, UV-36, and UV-37.
6. Provide regulation and control of the discharge flow of AF Pumps #1 and #2 to the SG system with HV-30, HV-31, HV-32, and/or HV-33.
7. Provide local indication and control room indication of AF Pump #1 discharge pressure and annunciate in the control room on low discharge pressure.
8. Provide local indication and control room indication of AF Pump #2 discharge pressure and annunciate in the control room on low discharge pressure.
9. Provide control room indication of AF Pump #3 discharge pressure and annunciate in the control room on low discharge pressure.
10. Provide indication of essential AF system flow to the SG system in the control room and at the remote shutdown panel and redundant indication at the technical support center.
In Interfaces:
1. AC and DC power. 2. Hydrazine and ammonia from the SC system. 3. Water from the CT system. 4. Water from the CH system.

Table C-2

COMPONENT MISSION TIME AND DEMAND CYCLE

AF System	
AF Pump #1	216 hours operation 27 starts
AF Pumps #2 and #3	96 hours operation 24 starts

C-2. (The complete fault tree model for the AF system is not given in this report.)

The Importance Ranking of each component was determined by measuring the changes in the probability of a functional failure, assuming the component is perfectly reliable versus the reliability using available data. This measures to what degree the reliability of a single component can improve the reliability of performance of function, and is called the Fussell-Vesely importance measure. It was this importance measure that was used to rank a component's importance within a system in terms of failure probability.

The Importance Ranking for each component was determined but is not given in this report. Those component failure modes with a Fussell-Vesely importance measure greater than 1.0E-2 were ranked E_H, or high. Importance measures less than 1.0E-2 and greater than 1.0E-3 were ranked E_M, or medium, and measures less than 1.0E-3 and greater than 1.0E-5 were ranked E_L, or low. Failure modes with an importance measure of less than 1.0E-5 were determined to be insignificant and no longer considered in the evaluation. Comparison of the importance rankings determined by the RCM study with the list of AF system risk-critical components developed in Appendix A reveals almost complete agreement. The only disagreement was the inclusion of manual valves and handswitches in the RCM study, which were not identified as risk-critical components. These components were at the bottom of the importance rankings.

To help ensure that the fault tree models were correct and the Fault Tree Analysis was complete and thorough, two additional information collection tasks were performed.

A) The CM histories for the AF system were reviewed to: 1) identify applicable and available plant-specific component failure rate data and 2) identify those actual system or component failures that may not have been evident in the Fault Tree Analysis and that may provide

additional information for a later determination of failure modes.

B) AF system PM plans and surveillance tests were also reviewed to provide a comparison of present PM and surveillance activity, and those components ranked important in the Fault Tree Analysis.

C.4 CORRECTIVE MAINTENANCE REVIEW

The AF system CM histories for all units of the cooperating plant site were reviewed. Because of the large amount of CM activity that was directly or indirectly the result of new construction or post-construction maintenance, CM histories were reviewed from the date of commercial operation to the present. CM histories from all units were reviewed because this provided more information regarding system performance and failures. A close review of this information, coupled with interviews with plant maintenance staff and systems engineers, provided several insights. For example:

AF System

- The AF system has experienced a high CM load.
- Most of the recurring CM activity is directed towards pumps and valves, with particular emphasis on repairing motor-operated valves, reworking manual valves, and adjusting packing or repacking pumps and valves.
- It should be noted that, whereas the number of CM tasks on motor-operated valves is high, this may be the result of a successful motor-operated valve condition-monitoring program, which uncovers failures that are then corrected by CM tasks.

The CM review did not identify any unique functional failures or failure modes that had not been considered in the fault tree model. It did, however, confirm some of the results of that mode, and also confirmed that pumps, valves, and, to a less extent, instrumentation, are the principal contributors to failed system performance.

C.5 PREVENTIVE MAINTENANCE REVIEW

As stated in Section C.2, the PM plans were reviewed to assure a complete study. A complete summary of the current PM program for the AF system is not given in this report. Plan reviews and maintenance staff interviews provided the following information:

- Of the 67 tasks identified as being performed, 40 are also identified as a technical specification requirement,

a regulatory commitment, an FSAR requirement, or as supporting a surveillance test.

- Management recognizes the use of condition monitoring, and already has several condition-monitoring programs in place.

- Several time-directed PMs are still being prepared but are not yet approved and therefore, were not considered in this study.

- Several primarily time-directed and replacement-oriented PMs are being written and implemented in response to the environmental qualification program. The validity or justification for qualification maintenance was not addressed in this study.

- The PM plan is in a constant process of evaluation and change as plant operating and maintenance experience is gained. Because the PM plan is subject to change, the plan as it existed approximately one year ago was used for review.

The PM plan review revealed that the PM load is high. A comparison of PM load to CM load indicates that PM load is much higher.

C.6 SURVEILLANCE TESTS AND LICENSE COMMITMENTS

C.6.1 Surveillance Tests

The surveillance tests for the AF system were also reviewed. A complete summary of the surveillance tests is not given in this report. The review indicated that safety-related equipment operability is addressed through performance of a surveillance test, and operability of other than safety-related equipment is addressed through performance of a PM task.

C.6.2 License Commitments

License commitments applicable to the AF system were reviewed. Where specific commitments could be identified, the commitment number was noted under Special Notes in the Preventive Maintenance Summary (which is not given in this report).

C.7 EVALUATION OF FAILURES USING FAILURE MODES AND EFFECTS ANALYSIS

Based on the effects each failure mode analyzed would have locally, on the system and on the plant, the criticality of component failure within the system can be assigned.

This is accomplished by reviewing the three-page RCM methodology flow chart (Figure C-1). It can be seen that the criticality of the component failure is determined based on a combination of importance ranking (page 1 of the flow chart) and the response to specific effect questions addressed in the flow chart (page 2 of the flow chart). As can be seen by reviewing the flow chart, failure mode effect questions are dependent upon the importance rank. Since there are three importance ranks (E_H, E_M, E_L), three different FMEA forms were developed. An example of each FMEA form can be found in Tables C-3, C-4, and C-5. The resulting criticality assigned to each component, based on the failure modes analyzed through Fault Tree Analysis, FMEA, and the RCM flow chart can also be found on the FMEA forms.

C.8 PM TASK SELECTION

After the criticality of each component and functional failure was identified, and the failure modes noted, PM task selection appropriate to the functions and requirements of the system was possible. When criticality rankings determined through the RCM flow diagram (Figure C-1) indicated that a functional failure has a LOW criticality, PM task selection was generally not necessary. However, if the functional failure was identified as MEDIUM or HIGH criticality, page 3 of the RCM methodology flow diagram was used to prioritize those applicable and effective PM tasks that might prevent the failure.

When identifying specific RCM-oriented PM tasks and an overall well-designed PM program, the goals of the RCM analysis should be kept in mind. A maintenance program based on RCM methodology should cost-effectively focus maintenance efforts on maintaining system function by:

- Identifying as many applicable and effective actions as possible that will preclude CM.
- Placing an emphasis on condition-monitoring tasks that monitor and trend specific equipment characteristics (such as vibration, flow, oil analysis, etc.) for correlation against an established set of criteria indicating future functional failure.
- Focusing PMs on critical components and their dominant failure modes.
- Eliminating PM tasks determined to be unnecessary due to the fact that the tasks are not applicable or cost-effective, or that the failure mode being prevented is not of sufficient importance to warrant PM.

Table C-3
SAMPLE FMEA - E_H

FAILURE MODES AND EFFECTS ANALYSIS							AF System	
FUNCTION: Provide water to steam generators on demand					IMPORTANCE RANK: E_H		PAGE: 1 of 6	
FUNCTIONAL FAILURE: Failure to provide water to steam generators on demand								
DOMINANT FAILURE MODES	FAILURE EFFECTS DESCRIPTION			LOSS OF FUNCTION, CAUSE DAMAGE, OR AFFECT SAFETY?	PREVIOUSLY CAUSED FORCED OUTAGE?	LIKELY TO CAUSE FORCED OUTAGE?	AFFECT SYSTEM PERFORM-ANCE?	CRITICALITY
	LOCAL	SUBSYS/SYS	PLANT					
3.1.1 Pump AFN-P01 fails to continue to run	Loss of AF system N train flow.	Loss of N train flow to the SG system. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	No	Yes	--	High
3.1.2 Pump AFB-P01 fails to continue to run	Loss of AF system B train flow.	Loss of B train flow to the motor-operated regulating and isolation valves. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	No	Yes	--	High
3.1.3 Pump AFA-P01 fails to start	Loss of AF system A train flow.	Loss of A train flow to the motor-operated regulating and isolation valves. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	Yes	--	--	High
3.1.4 Pump AFN-P01 fails to start	Loss of AF system N train flow.	Loss of N train flow to the SG system. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	No	Yes	--	High
3.1.5 Pump AFA-P01 fails to continue to run	Loss of AF system A train flow.	Loss of A train flow to the motor-operated regulating and isolation valves. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	Yes	--	--	High
3.1.6 Pump AFB-P01 fails to start	Loss of AF system B train flow.	Loss of B train flow to the motor-operated regulating and isolation valves. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	No	Yes	--	High
3.1.7 Motor valve HV54 fails to open	No steam is supplied to start AFA-P01.	Pump AFA-P01 fails to start on demand. Loss of A train flow to the motor-operated regulating and isolation valves. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	No	Yes	--	High
3.1.8 Motor valve UV35 fails to open	AF system train B flow to B steam generator is blocked.	Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected. Failure to meet technical specification 3.6.3; if the valve is not operable within 4 hours, plant operation mode may be affected	No	No	Yes	--	High

Table C-4
SAMPLE FMEA - E_M

FAILURE MODES AND EFFECTS ANALYSIS							AF System
FUNCTION: Provide water to steam generators on demand					IMPORTANCE RANK. E_M		PAGE: 4 of 6
FUNCTIONAL FAILURE: Failure to provide water to steam generators on demand							
DOMINANT FAILURE MODES	FAILURE EFFECTS DESCRIPTION			LOSS OF FUNCTION, CAUSE DAMAGE, OR AFFECT SAFETY?	PREVIOUSLY CAUSED FORCED OUTAGE?	LIKELY TO CAUSE FORCED OUTAGE?	CRITICALITY
	LOCAL	SUBSYS/SYS	PLANT				
3.1.19 Failure of handswitch HS10	Loss of control room control of AFB-P01.	No manual backup to start AFB-P01 in the event pump does not start on AFAS.	None	No	No	No	Medium
3.1.20 Check valve V015 fails to open	AF system train A flow is blocked at AFA-P01 discharge.	Loss of A train flow to the motor-operated regulating and isolation valves. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	No	Yes	High
3.1.21 Check valve V137 fails to open	AF system train A flow is blocked at AFA-P01 discharge.	Loss of A train flow to the motor-operated regulating and isolation valves. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	No	Yes	High
3.1.22 Check valve V079 fails to open	AF system train A and B flow to steam generator A is blocked.	Loss of one redundant flow path to steam generator A.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	No	Yes	High
3.1.23 Check valve V080 fails to open	AF system train A and B flow to steam generator B is blocked.	Loss of one redundant flow path to steam generator B.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	No	Yes	High
3.1.24 Manual valve V025 fails to remain open	AF system train B flow is blocked at AFN-P01 discharge.	Loss of B train flow to the motor-operated regulating and isolation valves. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	No	Yes	High
3.1.25 Manual valve V013 fails to remain open	AF system train N flow is blocked at AFN-P01 discharge.	Loss of N train flow to the SG system. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	No	Yes	High
3.1.26 Manual valve V001 fails to remain open	AF system train N flow is blocked at the suction of AFN-P01.	Possible damage to AFN-P01 due to lack of suction flow. Loss of N train flow to the SG system. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	No	No	Yes	High

Table C-5
SAMPLE FMEA - E_L

FAILURE MODES AND EFFECTS ANALYSIS							AF System	
FUNCTION: Provide water to steam generators on demand					IMPORTANCE RANK: E_L		PAGE: 5 of 6	
FUNCTIONAL FAILURE: Failure to provide water to steam generators on demand								
DOMINANT FAILURE MODES	FAILURE EFFECTS DESCRIPTION			AFFECT SYSTEM PERFORM-ANCE?	LOSS OF FUNCTION, CAUSE DAMAGE, OR AFFECT SAFETY?	PREVIOUSLY CAUSED FORCED OUTAGE?	LIKELY TO CAUSE FORCED OUTAGE?	CRITICALITY
	LOCAL	SUBSYS/SYS	PLANT					
3.1.27 Failure of handswitch HS [illegible] (A, B, C or D)	Control of UV34 is reduced to triple redundant.	None	None	No	--	--	--	Low
3.1.28 Failure of handswitch HS31 (A, B, C or D)	Control of HV31 is reduced to triple redundant.	None	None	No	--	--	--	Low
3.1.29 Failure of handswitch HS35 (A, B, C or D)	Control of UV35 is reduced to triple redundant.	None	None	No	--	--	--	Low
3.1.30 Failure of handswitch HS30 (A, B, C or D)	Control of HV30 is reduced to triple redundant.	None	None	No	--	--	--	Low
3.1.31 Manual valve V002 fails to remain open	No steam is supplied to operate AFA-P01.	Without operator action to open V055, AFA-P01 will not operate. Loss of A train flow to the motor-operated regulating and isolation valves. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	Yes	No	No	Yes	High
3.1.32 Manual valve V016 fails to remain open	AF system train A flow is blocked at AFA-P01 discharge.	Loss of A train flow to the motor-operated regulating and isolation valves. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	Yes	No	No	Yes	High
3.1.33 Motor valve HV54 fails to remain open	Steam supply to operate AFA-P01 is blocked.	Pump AFA-P01 fails to continue to run. Loss of A train flow to the motor-operated regulating and isolation valves. Loss of AF system triple redundancy.	Failure to meet technical specification 3.7.1.2; if not repaired within 72 hours, plant operation mode may be affected.	Yes	No	No	Yes	High
3.1.34 Failure of handswitch HS33 (A, B, C or D)	Control of HV33 is reduced to triple redundant.	None	None	No	--	--	--	Low
3.1.35 Failure of handswitch HS32 (A, B, C or D)	Control of HV32 is reduced to triple redundant.	None	None	No	--	--	--	Low
3.1.36 Failure of handswitch HS36 (A, B, C or D)	Control of UV36 is reduced to triple redundant.	None	None	No	--	--	--	Low
3.1.37 Failure of handswitch HS37 (A, B, C or D)	Control of UV37 is reduced to triple redundant.	None	None	No	--	--	--	Low
3.1.38 Manual valve V106 fails to remain closed	Leakage from AF system. Water hazard.	None	None	No	--	--	--	Low

- Identifying time-directed PM tasks that are applicable if the probability of failure increases with time and the failure is not indicated in advance.

- Identifying failure-finding tasks that discover otherwise hidden and non-preventable failures.

- Extending existing time-directed task intervals through the age exploration process or frequency optimization.

- Addressing design change and run-to-failure options.

In order to develop PM tasks that address the MEDIUM and HIGH criticality failures and that are responsive to the goals of the PM program and RCM methodology, Figure C-1 was referred to. For each failure mode, the appropriate responsive PM task was defined as either condition-directed, time-directed, or failure-finding. PM actions were then identified for each failure mode. The complete table of PM task selections, which is not given in this report, was then used in the development of the component-specific PM task recommendations. (Examples are discussed in paragraph C.10.1).

Several condition-monitoring activities are already in place at the plant site, and condition-monitoring tasks were identified as appropriate for some components, including:

- Motor-operated valves

- Pumps

- Heat exchangers

Effective implementation of condition-directed maintenance requires monitoring and/or trending activities to be defined that will provide indications of pending functional failure. For many components, the use of condition-monitoring activities to preclude time-directed maintenance can be effectively supplemented by a rigorous visual inspection program.

The use of condition-monitoring also implies the necessity for data collection and trending. For all those parameters trended, such as vibration analysis, oil sample analysis, or heat exchanger performance, baseline values must be established for each monitored component and values established that will initiate the condition-directed maintenance. However, for condition-monitoring tasks and condition-directed maintenance to be effective, the man-hours and costs expended on data collection and trending must be cost-effective when compared to the replaced time-directed maintenance.

The plant site has already established several condition-monitoring and/or trending programs, including:

- Vibration analysis
- Lube oil analysis
- Heat exchanger performance monitoring
- Filter differential pressure monitoring
- Motor-operated valve monitoring program

In addition, several other monitoring programs are available or in place within the industry to support the initiation of condition-directed maintenance; however, they are not yet considered part of a coordinated condition-monitoring program at the plant site.

Acoustic Monitoring

Acoustic monitoring is an informal condition-monitoring program in the early stages of development. The program could be developed to assist in the detection of valve leakage and check valve failure. Specific applications of available technology are still being evaluated. As a condition-monitoring program, acoustic monitoring could help to identify valve performance loss and eliminate unnecessary valve maintenance.

Thermographic Monitoring

Thermographic condition monitoring, primarily of electrical components, is a newly-evolving technology and is still unknown in terms of its preventive maintenance applications. Thermographic monitoring has also prove useful in the identification of failed or leaking valves.

C.9 PLANT INTERVIEWS

In order to collect additional information that could be useful in the PM task selection and identification, interviews were conducted with the plant's maintenance personnel and systems engineers. Each interview lasted about an hour. The interviews were conducted on a one-on-one basis, and they were purposely informal to create an easy atmosphere for information exchange. Most of the discussion focused on the list of questions identified in Table C-6. The primary goal was to gain additional insights into present maintenance practices, collect knowledge about equipment problems that goes beyond the written records, and identify applicable information that may have been missed or overlooked.

Significant information obtained as a result of the interviews included:

Table C-6

INTERVIEW QUESTIONS

History of the system in terms of operational experience and problems, design problems, failures ... 1) component maintenance problems? 2) component design problems? 3) component operational problems?
What is the basis for maintenance frequency and that maintenance which is done?
Is root-cause analysis performed on equipment failures?
What is involved in the vibration analysis: 1) trending - who? 2) consistent monitor points? 3) trained personnel?
Do inspections involve parts replacement and/or reworking of components?
Is post-maintenance verification testing done?
What are your personal opinions relating to equipment failure and causes, as well as strengths and weaknesses in current program practices?
Are there changes from the established normal practices in the operation, maintenance testing or environmental conditions that may have contributed to a change in equipment performance or reliability?
Do you have any opinions concerning the impact of the human factors issues involved in the maintenance activities? (This area will primarily deal with the design for maintenance on and equipment and system/building level. Other human factors issues may include the procedures, tools, lighting, hours, and general work conditions.
Can you offer any qualitative assessments of relative maintenance costs associated with various component types for each of the candidate systems?
Are there any maintenance activities now being done that you feel are not cost-effective, or activities that aren't being done and should be?

General Information

- Several condition-monitoring and trending programs are in place. These include oil sample analysis, vibration analysis, the trending of heat exchanger performance data, and the motor-operated valve monitoring program.
- There are no PM tasks to monitor pumps with packing for leaks. Although Operations tours could note packing leaks on logs, only maintenance should adjust pump packing.
- Qualification training is required for most maintenance, but the qualifications may not get renewed over long periods of time. Qualification training should be periodically renewed.
- There are no means to transfer technology and experience between maintenance crews from unit to unit except at the supervisor level
- One problem which seems prevalent is grease in motor-operated and manual gear valves.
- The oil analysis laboratory apparently does not provide indications with the oil sample results as to what acceptable levels of contaminants might be.
- There is a plant-wide problem with valves with reach rods. The reach rod clutch settings change, and there is no maintenance to address correcting them.
- Not all motor-operated valves are entered in the motor-operated valve monitoring program.
- Meggering heaters and motors serves no predictive purpose and is not generally encouraged.

AF System

- The AF system pumps have mechanical seals rather than packing, and very few problems have been encountered.
- There is no procedure and no acceptance criteria to perform motor air gap measurements.
- The lube oil filter for the turbine-driven pump has never been changed, but a maintenance task has recently been written to address this.

C.10 RESULTS: COMPARISON OF RECOMMENDATIONS WITH CURRENT PM PROGRAM

As noted in the RCM study, the Auxiliary Feedwater System (AF) analyzed is a safety-related system subject to technical specifications. The effect of proper preventive and corrective maintenance on this system has a direct impact on plant operation and safety. Therefore, the benefits derived from reliability-centered maintenance studies on such systems are quite subtle, and recommended maintenance activity changes are not easily undertaken when changes to technical specification or regulatory commitments are also considered.

From the utility's perspective, the results of this study indicate that, through the application of reliability-centered maintenance, preventive maintenance man-hours can be more efficiently optimized. For example, several maintenance tasks were identified that were recommended to be deleted, modified, or changed to condition-directed and one time-directed task was recommended to be added. Overall, the total time-directed preventive maintenance workload on the AF system would be changed from 67 time-directed tasks to 61, and the number of condition-directed preventive maintenance tasks would be increased from zero to seven. For the purposes of risk-focused maintenance, however, only 11 risk-critical components and their associated tasks were impacted, (i.e., modified). Due to the redundancy in system design, these 11 tasks represent only 3 types of component tasks. Table C-7 summarizes the recommendations of the RCM study of the AF system and contrasts these results with those for the identified risk-critical components only.

Table C-7

AF SYSTEM RCM RECOMMENDATIONS:
SYSTEM-WIDE AND RISK-CRITICAL COMPONENTS ONLY

	Total Number of Original PM Tasks	Tasks Modified	Tasks Added	Tasks Deleted
AF System	67	12	1	7
AF System Risk-Critical Components Only	33	11 *	0	0

* Ten time-directed tasks modified with portions changed to condition-directed.

Most of the components addressed in the following discussion were identified as HIGH or MEDIUM criticality. However, RCM analysis, as shown in Figure C-1, suggests that even for highly-critical

components, time-directed tasks may not always be appropriate. More specific discussion regarding the recommended PM program changes are given below. While not specifically quantifiable, following the recommendations is expected to result in lower corrective-maintenance activities in the future. (It should be noted that a condition-directed task necessarily requires a time-directed inspection task or some form of monitoring activity to initiate the task. Thus, instead of initiating maintenance every time-directed performance interval, the equipment performance is monitored and maintenance is called for when established standards are exceeded, possibly allowing one or more intervals to be passed without administrative approval.)

C.10.1 Motor-Operated Valves

One non-risk-critical MOV, which is not presently monitored through the motor-operated valve monitoring program, is recommended to be added to the that program.

All of the AF system motor-operated valves, including eight risk-critical MOVs, have time-directed maintenance tasks that reference one of two maintenance procedures. Both maintenance procedures include the use of meggering. Discussions with plant maintenance personnel, previous RCM study results, and input by industry maintenance experts support the contention that meggering is of little value except when installing or modifying equipment. Additionally, meggering does not serve well as a predictive tool. Meggering is recommended to be deleted from the tasks.

The remainder of the time-directed tasks that reference the two maintenance procedures address such maintenance as:

- Lubrication of the main gear box (a maintenance qualification program item)
- Measurement of stem diameter, pitch, and lead
- Motor operator and valve inspection
- Gear box grease relief inspection (a maintenance qualification program item)
- Various limit switch inspections (a maintenance qualification program item)
- Various torque switch inspections

The time-directed verification and inspection of lubrication, as a maintenance qualification program item, is recommended to be retained. However, the remainder of this maintenance task is recommended to be initiated only on a condition-directed basis, based upon the results of the motor-operated valve monitoring

program test results and system motor-operated valve surveillance tests.

C.10.2 Pumps and Motors

Motor air gap measurements are supposed to be conducted on a time-directed basis on motor-driven pumps #2 and #3 (risk-critical). There are no procedures on vendor acceptance criteria to conduct these measurements. Until such time as specific procedures and acceptance criteria are provided by the vendor, it is recommended that this maintenance activity be deleted. Motor air filter inspection is recommended to be retained on a time-directed basis.

C.10.3 Other Non-Risk-Critical Components

Several AF system manual valves receive time-directed maintenance to inspect, clean, lubricate, and stroke them. This maintenance activity is in response to IE86-61, addressing valve failures at Rancho Seco. One manual valve is stroked on a monthly basis through performance of system surveillance tests. Inspection, lubrication, and cleaning of this valve can be initiated as corrective maintenance based on operator observation. Therefore, the time-directed maintenance task on this valve is recommended to be deleted.

As the result of PM review, it should be noted that the PM task frequencies to calibrate pressure loops for pump #1 and pump #2 discharge pressures are inconsistent. The instrument loop calibration frequency for pump #1 is once per refueling, while the pump #2 frequency is once every two years.

Specific handswitch indicating bulbs at the remote shutdown panel are replaced on a time-directed basis. The status of these bulbs and their ability to function as required can be checked on a monthly basis through the performance of four surveillance tests. Even though replacement of these bulbs is identified as part of the qualification maintenance program for panel JZJAE01, these tasks are recommended to be deleted.

C.10.4 General Comments

Motor-Operated Valves

Under the present maintenance program, when motor-operated valve operators need refurbishment or servicing, the work is generally done at the valve station. Although not specifically recommended as a result of this RCM analysis, an alterative approach might include removing a valve operator that needs servicing, replacing it with an operator previously serviced, and then working on the operator off-line. This approach would require additional valve operator spare parts, but would likely reduce maintenance man-hours expended.

Interviews with maintenance personnel suggest that additional PM-related comments about motor-operated valves are warranted:

- Greasing of valve operators sometimes causes more problems than it prevents. Maintenance personnel sometimes approach this task with the idea that if a little is good, a lot is better. The net effect of this approach is deterioration of valve performance.

Oil Analysis

Oil samples are presently sent to an off-site laboratory for analysis. When the results are returned, out-of-specification values are not red-flagged, and the analysis results provide no indication as to the acceptability of the measurements. In order for an oil sample analysis program to be of use, acceptance criteria must be established for each component sampled, and sample results must be compared against these criteria. Analysis results should also be trended to indicate and identify slowly-developing problems.

REFERENCE

C-1. "Demonstration of Reliability-Centered Maintenance, Vol. 2: First Annual Progress Report from San Onofre Nuclear Generating Station", (EPRI-6152), Interim Report, September, 1989.

APPENDIX D

DEMONSTRATION OF RELIABILITY-FOCUSED MAINTENANCE FOR A NORMALLY OPERATING SYSTEM

D.1 INTRODUCTION

This appendix contains the demonstration of the reliability-focused maintenance (RFM) process for components in a normally operating system. For the purposes of this demonstration, a Reliability-Centered Maintenance study was used which was performed for the Feedwater (FW) System in a BWR plant at the request of the cooperating utility. The recommendations from the RCM study for the risk-critical components of the Feedwater System, which were determined in Appendix B by using the plant's PRA, are highlighted.

In general, the discussion in Appendix C, "Demonstration Of Reliability-Focused Maintenance For Standby Components", Section C1.1 and C1.2, is applicable to this demonstration. The system and component boundary issues specific to the Feedwater System of the BWR plant in this demonstration primarily involve the Condensate System (e.g., condensate booster pumps, check valves, etc.). For the reasons discussed in Section C.1.2, these components were not analyzed in the FW RCM study. However, unlike the RCM study of Appendix C, the "critical" components identified in this RCM study are not in complete agreement with the risk-critical component list developed in Appendix B. This disparity is due primarily to the fact that the RCM study was performed for the normally operating function of the FW system rather than for the specific function of the FW system which must be performed in response to an accident. Although the RCM study approach is appropriate for finding the dominant causes of the "Loss of Feedwater" initiating event, the system function definition used in the RCM study results in the identification of several components which do not serve any useful function in the FW system response to accidents (e.g., zinc injection pumps). (In addition, the utility made use of a PRA modeling technique of incorporating the lube oil pumps within the main feedwater pumps' component boundaries. Hence, lube oil pumps were not identified as risk-critical components.)

Similar disparities in results for component "criticality" would be expected for other normally operating systems. In results of this particular FW RCM study, the overlap with risk-critical components from Appendix A is sufficient for the purposes of risk-focused maintenance. However, it is recommended that the appropriateness of using traditional RCM studies for normally operating systems be justified by a similar comparison of "critical" and risk-critical component lists or by some other means.

D.2 SYSTEM BOUNDARY DEFINITION AND PARTITION

The system boundaries were defined for the FW system in the RCM analysis. System boundary definition is particularly important when RCM analysis is intended for eventual application on a plant-wide basis or when RCM analysis may be performed on interfacing systems. Strict boundary control and definition avoids analysis overlaps and gaps. The system boundaries for the FW system include:

- FW system side, as denoted in system drawings, of piping and valves which connect with the condensate system.
- The inlets to both condensers from the reactor feedwater pump recirculation lines.
- The inlet to condenser #2 from the HP heaters crosstie.
- The inlet to the reactor vessel at the feedwater inlet penetrations.
- The inlet to the feedwater system from the reactor water cleanup system.
- The inlet to the feedwater system from the control rod drive system.
- The FW system side of instrument air signals and control signals generated by other systems based on the status of those systems.
- The load side of switchgear for FW system power-operated equipment.
- The inlet to the HVAC exhaust from the casing vent pump common discharge header.

D.3 FAULT TREE ANALYSIS

Once the system boundaries were identified, the system was modeled for fault tree analysis. The FW system model was based upon system and component function, unique and vital for the operation of the system as a whole. Through fault tree analysis, each component within a system was evaluated to identify its functional significance. This system-level fault tree analysis provided the means whereby the failure modes for each defined component and function were identified, evaluated, and ranked in terms of importance.

The fault tree analysis provides a logical display of how component failures relate to cause a failure of function. The probability of failure of function was determined by using this logical display,

i.e., the fault tree model, quantified with available failure rate data and mission time for each component. Failure rate data was taken from IEEE STD 500 - 1084, "Reliability Data" and other sources, and supplemented by plant-specific information when available.

Most failure rate data available to the nuclear industry (including that used in this report) is based upon the demand scenarios developed in a PRA model. This failure data is not altogether appropriate for use in an RCM analysis where components may run continuously, or near-continuously, from refueling outage to refueling outage, or where a component is started and stopped daily. Therefore, the failure rate data used in the RCM analysis of the FW system was modified if the result of failure rate multiplied by mission time clearly fell outside the bounds of realism. As plant-specific failure rate data continues to be developed over time, the fault tree model can be updated and modified as appropriate.

Each component's mission time, test interval, and demand cycle were based on plant-specific system operating requirements through a period of 365 days. The system operating requirements that were used in this analysis can be found in Table D-1.

The mission times for other components within each system were based on that component's exposure to system operation, which is a function of the component's relationship to the equipment in Table D-1. (The complete fault tree model for the FW system is not given in this report.)

The Importance Ranking of each component was determined by measuring the changes in the probability of a functional failure, assuming the component is perfectly reliable versus the reliability of performance of function, and is called the Fussell-Vesely importance measure. It was this importance measure that was used to rank a component's importance within a system in terms of failure probability.

The Importance Ranking for each component was calculated but is not given in this report. Those failure modes with a Fussell-Vesely importance measure greater than 1.0E-2 were ranked E_H, or high. Importance measures less than 1.0E-2 and greater than 1.0E-3 were ranked E_M, or medium, and measures less than 1.0E-3 and greater than 1.0E-5 were ranked E_L, or low. Failure modes with an importance measure of less than 1.0E-5 were determined to be insignificant and no longer considered in the evaluation. Comparison of the importance rankings calculated in the FW RCM study with the list of risk-critical component derived from the PRA used in Appendix B revealed less agreement than was found in a similar comparison in Appendix C. There is agreement on the importance and risk-criticality of the feedwater regulating valves and main feedwater pump but other identified risk-critical

TABLE D-1

COMPONENT MISSION TIME AND DEMAND CYCLE

FW System	
Main Feedwater Pump #1	5780 hours operation 10 starts
Main Feedwater Pump #2	5780 hours operation 10 starts
Main Feedwater Pump #3	5790 hours operation 10 starts
Casing Vent Pump #1	4380 hours operation
Casing Vent Pump #2	4380 hours operation
Zinc Injection Pump #1	4380 hours operation
Zinc Injection Pump #2	4380 hours operation
Block Valve #1	8 open/close demands
Block Valve #2	8 open/close demands
Block Valve #3	8 open/close demands
Feedwater Regulating Valve #1	8660 hours flow control 8 open/close demands
Feedwater Regulating Valve #2	8660 hours flow control 8 open/close demands
Feedwater Regulating Valve #3	8660 hours flow control 8 open/close demands

components are spread throughout the importance rankings. The reasons for this disparity in results were discussed in Section D-1.

To help ensure that the fault tree models were correct and the fault tree analysis was complete and thorough, two additional information collection tasks were performed.

A) The CM histories for the FW system were reviewed to: 1) identify applicable and available plant-specific component failure rate data and 2) identify those actual system or component failures that may not have been evident in the Fault Tree Analysis, and that may provide additional information for a later determination of failure modes.

B) FW system PM plans and surveillance tests were also reviewed to provide a comparison of present PM and surveillance activity and those components ranked important in the Fault Tree Analysis.

D.4 CORRECTIVE MAINTENANCE REVIEW

The CM histories for the FW system were reviewed. The easily-accessible CM data provided information from October 1984 to present. This provided nearly six years of operation information regarding system performance and failures. In addition, the Nuclear Plant Reliability Data System (NPDRS) was accessed and provided information on significant FW system component failures from 1974 to the present. Also, the plant-specific Baseline Events Analysis Reliability Data system (BEARDS) was accessed and provided information on FW system component failures that resulted in a forced outage or forced power reduction. This information was provided from 1971 to the present. (A complete listing of the relevant CM summary, the NPRDS summary, and a summary of the BEARDS data were given in the original RCM report but are not given here.) A close review of this information coupled with interviews with plant maintenance staff and systems engineers, provided several insights. For example:

<u>FW System</u>

- The FW system has experienced a moderate CM load.
- Most of the recurring CM activity is directed towards pumps and valves, with particular emphasis on repairing the feed regulating valves, reworking manual valves, and adjusting packing or repacking valves.
- Failures of the feed regulating valves have resulted in 22 forced outages or power reductions in the last 19 years.

- A significant number of feed regulating valve failures have involved failure or malfunction of the positioner.

- Check valve failures and resulting loose parts have also contributed to feed regulating valve malfunctions.

The CM review did not identify any unique functional failures or failures modes that had not been considered in the fault tree model other than loose parts within the system contributing to valve malfunction. It did, however, confirm some of the results of that model and also confirmed that pumps, valves, and, to a lesser extent, instrumentation, are the principal contributors to failed system performance.

D.5 PREVENTIVE MAINTENANCE REVIEW AND SURVEILLANCE TEST REVIEW

As stated in Section D.3, the PM plans were reviewed to assure a complete study. (A summary of the current PM program for the FW system was given in the original report but is not given here.) Plan reviews and maintenance staff interviews provided the following information:

- Management recognizes the use of condition monitoring, and already has several condition-monitoring programs in place.

- The PM plan is in a constant process of evaluation and change as plant operating and maintenance experience is gained. Because the PM plan is subject to change, the plan as it existed in July 1990 was used for review.

- A complete review of PM activity was difficult because components of the FW system were identified in the maintenance work records as either in the Feedwater System, the Condensate System, the Feedwater Coolant Injection System, or miscellaneous.

- Surveillance tests which address safety-related component operability or the operability of components subject to technical specifications, are tracked and scheduled manually.

- Each department (e.g., Engineering, Operations, Maintenance, and I&C) has its own maintenance and testing program. There is little communication between departments addressing maintenance and testing activities.

- There appear to be no PM tasks assigned to address Equipment Qualification replacement requirements.

- There are a large number of manual valves that are subject to time-directed maintenance inspections.

The PM plan review revealed that the PM load is high. A comparison of PM load to CM load indicated that PM load is higher.

D.6 EVALUATION OF FAILURES USING FAILURE MODES AND EFFECTS ANALYSIS

For each of the failure modes identified in the fault tree analysis that had an Importance Rank of E_H, E_M, E_L, a Failure Modes and Effects Analysis (FMEA) was performed. This analysis coupled the significant failure modes with each functional failure and identified the effects of the failure locally, on the system and on the plant. For the FW system, the following failure was defined:

FW System - Failure to provide controlled water flow to the reactor on demand.

Based upon the local effects of each failure mode analyzed, the criticality of component failure within the system can be assigned. This is accomplished by reviewing the three-page RCM methodology flow chart (see Appendix C, Figure C-1). It can be seen that the criticality of the component failure is determined based on a combination of importance ranking (page 1 of Figure C-1) and the response to specific effect questions addressed in the flow chart (page 2 of Figure C-1). As can be seen by reviewing the flow chart, failure mode effect questions are dependent upon the importance rank. Since there are three importance ranks (E_H, E_M, E_L), three different FMEA forms were developed. An example of each FMEA form can be found in Tables D-2, D-3, and D-4. The resulting criticality assigned to each component, based on the failure modes analyzed through Fault Tree Analysis, FMEA, and the RCM flow chart can also be found on the FMEA forms.

D.7 PM TASK SELECTION

After the criticality of each component and functional failure was identified, and the failure modes noted, PM task selection appropriate to the functions and requirements of the system was possible. When criticality rankings determined through the RCM flow diagram (Appendix C, Figure C-1) indicated that a functional failure has a LOW criticality, PM task selection was generally not necessary or required. However, if the functional failure was identified as being MEDIUM or HIGH criticality, page 3 of the RCM methodology flow diagram was used to prioritize those applicable and effective PM tasks that might prevent the failure.

Table D-2
SAMPLE FMEA - E_H

FAILURE MODES AND EFFECTS ANALYSIS								
FUNCTION: Provide controlled flow to the reactor on demand FUNCTIONAL FAILURE: Failure to provide controlled flow to the reactor on demand					IMPORTANCE RANK: E_H		FW System PAGE: 1 of 7	
DOMINANT FAILURE MODES	FAILURE EFFECTS DESCRIPTION			LOSS OF FUNCTION, CAUSE DAMAGE, OR AFFECT SAFETY?	PREVIOUSLY CAUSED FORCED OUTAGE?	LIKELY TO CAUSE FORCED OUTAGE?	AFFECT SYSTEM PERFORM-ANCE?	CRITICALITY
	LOCAL	SUBSYS/SYS	PLANT					
1. FW-5A fails to control flow	Loss of controlled flow through one of two redundant trains of regulating valves	Loss of flow control capability to the reactor	Reactor may be forced to reduce power or scram. Failure to meet technical specification 4.5.C.1.a. Plant in LCO.	Yes	--	--	--	High
2. FW-5B fails to control flow	Loss of controlled flow through one of two redundant trains of regulating valves	Loss of flow control capability to the reactor	Reactor may be forced to reduce power or scram. Failure to meet technical specification 4.5.C.1.a. Plant in LCO.	Yes	--	--	--	High
3. M2-10A fails to continue to run	Loss of flow from feed pump A train	Loss of feed pump 2-of-3 redundancy	Reactor may be forced to reduce power or scram if standby pump does not start. Failure to meet technical specification 4.5.C.1.a. Plant in LCO.	No	Yes	--	--	High
4. M2-10B fails to continue to run	Loss of flow from feed pump A train	Loss of feed pump 2-of-3 redundancy	Reactor may be forced to reduce power or scram if standby pump does not start. Failure to meet technical specification 4.5.C.1.a. Plant in LCO.	No	Yes	--	--	High
5. M2-10C fails to continue to run	Loss of flow from feed pump A train	Loss of feed pump 2-of-3 redundancy	Reactor may be forced to reduce power or scram if standby pump does not start. Failure to meet technical specification 4.5.C.1.a. Plant in LCO.	No	Yes	--	--	High
6. Lube oil pump M2-10A-1 fails to continue to run	Loss of standby and startup lubrication for the standby feedwater pump	Feed pump has no lubrication in standby. If started, bearings may seize.	Feed pump placed out of service. Loss of 2-of-3 feed pump redundancy.	No	No	No	No	Medium
7. Lube oil pump M2-10B-1 fails to continue to run	Loss of standby and startup lubrication for the standby feedwater pump	Feed pump has no lubrication in standby. If started, bearings may seize.	Feed pump placed out of service. Loss of 2-of-3 feed pump redundancy.	No	No	No	No	Medium
8. GEZIP pump M2-32A fails to continue to run	Loss of zinc flow from GEZIP tank	No zinc flow to feedwater and reactor	None	No	No	No	No	Medium
9. GEZIP pump M2-32B fails to continue to run	Loss of zinc flow from GEZIP tank	No zinc flow to feedwater and reactor	None	No	No	No	No	Medium
10. Lube oil pump M2-10C-1 fails to continue to run	Loss of standby and startup lubrication for the standby feedwater pump	Feed pump has no lubrication in standby. If started, bearings may seize.	Feed pump placed out of service. Loss of 2-of-3 feed pump redundancy.	No	No	No	No	Medium

Table D-3
SAMPLE FMEA - E_M

FAILURE MODES AND EFFECTS ANALYSIS							FW System
FUNCTION: Provide controlled flow to the reactor on demand FUNCTIONAL FAILURE: Failure to provide controlled flow to the reactor on demand					IMPORTANCE RANK: E_M		PAGE: 2 of 7
DOMINANT FAILURE MODES	FAILURE EFFECTS DESCRIPTION			LOSS OF FUNCTION, CAUSE DAMAGE, OR AFFECT SAFETY?	PREVIOUSLY CAUSED FORCED OUTAGE?	LIKELY TO CAUSE FORCED OUTAGE?	CRITICALITY
	LOCAL	SUBSYS/SYS	PLANT				
11. Failure of M2-10A electrical fault trips	Partial feed pump electrical trip protection is lost	If running, feed pump may not continue to run or may not trip on fault condition.	None	No	No	No	Medium
12. Failure of M2-10B electrical fault trips	Partial feed pump electrical trip protection is lost	If running, feed pump may not continue to run or may not trip on fault condition.	None	No	No	No	Medium
13. M2-10A lube oil system fails to maintain level or lubricate	Loss of bearing lubrication. Pump bearings may seize, causing pump failure	Potential feed pump failure. Loss of 2-of-3 feed pump redundancy	Reactor may be forced to reduce power or scram if standby pump does not start. Failure to meet technical specification 4.5.C.1.a. Plant in LCO.	Yes	--	--	High
14. M2-10B lube oil system fails to maintain level or lubricate	Loss of bearing lubrication. Pump bearings may seize, causing pump failure	Potential feed pump failure. Loss of 2-of-3 feed pump redundancy	Reactor may be forced to reduce power or scram if standby pump does not start. Failure to meet technical specification 4.5.C.1.a. Plant in LCO.	Yes	--	--	High
15. M2-31A fails to continue to run	Loss of feed pump casing vent vacuum	Loss of casing vent vacuum redundancy	If standby casing vent vacuum pump not started, airborne contamination may increase.	No	No	No	Medium
16. M2-31B fails to continue to run	Loss of feed pump casing vent vacuum	Loss of casing vent vacuum redundancy	If standby casing vent vacuum pump not started, airborne contamination may increase.	No	No	No	Medium
17. Flow loop 2-1 out of calibration or fails	Loss of reliable suction flow monitoring of M2-10A	Loss of reliable automatic control of FW-14A position	Loss of minimum flow recirculation control. Loss of partial FWCI control circuit. Failure to meet technical specification 4.5.C.1.b. Plant in LCO.	No	No	No	Medium
18. Flow loop 2-2 out of calibration or fails	Loss of reliable suction flow monitoring of M2-10B	Loss of reliable automatic control of FW-14B position	Loss of minimum flow recirculation control. Loss of partial FWCI control circuit. Failure to meet technical specification 4.5.C.1.b. Plant in LCO.	No	No	No	Medium
19. Flow loop 640 out of calibration or fails	Loss of reliable total feed flow indication and control input	Loss of accurate flow input to RFP protection and worth minimizer and other safety features	Reactor safety margin may be lowered.	Yes	--	--	High
20. FW-5C fails to control flow	Loss of automatic flow control during startup and low flow	To continue low flow operation, use of FW-5A or FW-5B is necessary	Failure to meet technical specification 4.5.C.1.a. Plant in LCO.	No	No	Yes	High

Table D-4
SAMPLE FMEA - E_L

FAILURE MODES AND EFFECTS ANALYSIS							FW System	
FUNCTION: Provide controlled flow to the reactor on demand FUNCTIONAL FAILURE: Failure to provide controlled flow to the reactor on demand					IMPORTANCE RANK: E_L		PAGE: 5 of 7	
DOMINANT FAILURE MODES	FAILURE EFFECTS DESCRIPTION			AFFECT SYSTEM PERFORMANCE?	LOSS OF FUNCTION, CAUSE DAMAGE, OR AFFECT SAFETY?	PREVIOUSLY CAUSED FORCED OUTAGE?	LIKELY TO CAUSE FORCED OUTAGE?	CRITICALITY
	LOCAL	SUBSYS/SYS	PLANT					
37. Heater M2-4A ruptures	Loss of feedwater flow volume. Contaminated water hazard	Decrease in water to the reactor. Partial loss of feedwater heating. Loss of heater train redundancy	Decrease in reactor water level. Partial LOCA condition.	Yes	Yes	--	--	High
38. Heater M2-4B ruptures	Loss of feedwater flow volume. Contaminated water hazard	Decrease in water to the reactor. Partial loss of feedwater heating. Loss of heater train redundancy	Decrease in reactor water level. Partial LOCA condition.	Yes	Yes	--	--	High
39. Heater M2-5A ruptures	Loss of feedwater flow volume. Contaminated water hazard	Decrease in water to the reactor. Partial loss of feedwater heating. Loss of heater train redundancy	Decrease in reactor water level. Partial LOCA condition.	Yes	Yes	--	--	High
40. Heater M2-5B ruptures	Loss of feedwater flow volume. Contaminated water hazard	Decrease in water to the reactor. Partial loss of feedwater heating. Loss of heater train redundancy	Decrease in reactor water level. Partial LOCA condition.	Yes	Yes	--	--	High
41. PS-2-24 out of calibration or fails	Loss of reliable pump start permissive control for M2-10C	M2-10C may not start on demand or start with inadequate suction pressure	None	No	--	--	--	Low
42. PS-2-39C out of calibration or fails	Loss of reliable pressure switch function based on M2-10C lube oil pressure	Loss of reliable pump start permissive and pump trip control. M2-10C may not start on demand or trip on lube oil pressure fault condition.	None	Yes	No	No	No	Medium
43. PS-2-40C out of calibration or fails	Loss of reliable pressure switch function based on M2-10C lube oil pressure	Motor-driven lube oil pump M2-10C-1 may not start on low lube oil pressure condition or stop on adequate lube oil pressure. Feed pump bearing damage may occur.	None	Yes	No	No	No	Medium
44. Check valve FW-9A fails to open or remain open	Train A flow to the reactor is blocked	Loss of partial flow to the reactor. Loss of redundant containment isolation valve redundancy	Reactor may be forced to reduce power or have forced outage. Failure to meet technical specification 4.5.C.1.a and 3.7.D.2. Plant in LCO.	Yes	Yes	--	--	High
45. Check valve FW-10A fails to open or remain open	Train A flow to the reactor is blocked	Loss of partial flow to the reactor. Loss of redundant containment isolation valve redundancy	Reactor may be forced to reduce power or have forced outage. Failure to meet technical specification 4.5.C.1.a and 3.7.D.2. Plant in LCO.	Yes	Yes	--	--	High

When identifying specific RCM-oriented PM tasks and an overall well-designed PM program, the goals of the RCM analysis should be kept in mind. A maintenance program based on RCM methodology should cost-effectively focus maintenance efforts on maintaining system function by:

- Identifying as many applicable and effective actions as possible that will preclude CM.
- Placing an emphasis on condition-monitoring tasks that monitor and trend specific equipment characteristics (such as vibration, flow, oil analysis, etc.) for correlation against an established set of criteria indicating future functional failure.
- Focusing PMs on critical components and their dominant failure modes.
- Eliminating PM tasks determined to be unnecessary due to the fact that the tasks are not applicable or cost-effective, or that the failure mode being prevented is not of sufficient importance to warrant PM.
- Identifying time-directed PM tasks that are applicable if the probability of failure increases with time and the failure is not indicated in advance.
- Identifying failure-finding tasks that discover otherwise hidden and non-preventable failures.
- Extending existing time-directed task intervals through the age exploration process or frequency optimization.
- Addressing design change and run-to-failure options.

In order to develop PM tasks that address the MEDIUM and HIGH criticality failures and that are responsive to the goals of the PM program and RCM methodology, Figure C-1, "RCM Methodology Process Diagram", (page 3 of the figure) was used. For each failure mode, the appropriate responsive PM task was defined as either condition-directed, time-directed, or failure-finding. PM actions were then identified for each failure mode. (The complete table of PM task selections is not given in this report. This table was then used in the development of the component-specific PM task recommendations.)

Several condition-monitoring activities are already in place at the plant site, and condition-monitoring tasks were identified as appropriate for some components, including:

- Motor-operated valves
- Pumps

- Heaters (heat exchangers)

Effective implementation of condition-directed maintenance requires monitoring and/or trending activities to be defined that will provide indications of pending functional failure. On many of the components, the use of condition-monitoring activities to preclude time-directed maintenance can be effectively supplemented by a rigorous visual inspection program.

The use of condition-monitoring also implies the necessity for data collection and trending. For all those parameters trended, such as vibration analysis, oil sample analysis, or heat exchanger performance, baseline values must be established for each monitored component, and values established that will initiate the condition-directed maintenance. However, for condition-monitoring tasks and for the implementation of condition-directed maintenance to be effective, the man-hours and costs expended on data collection and trending must be cost-effective when compared to the replaced time-directed maintenance.

The plant site has already established several condition-monitoring and/or trending programs applicable to FW components, including:

- Vibration analysis
- Lube oil analysis
- Heat exchanger performance monitoring
- Thermographic monitoring
- A motor-operated valve monitoring program

It should be noted that thermographic monitoring on FW system components is still only an informal program, used primarily for heat performance monitoring and identification of leaking valves such as the three parallel minimum flow recirculation valves. It is also occasionally used to monitor electrical components.

It should also be noted that although lube oil sample analysis is done on a quarterly basis for the feedwater pumps, the results of the analysis are not presently trended. In addition, another monitoring program is available or in place within the industry to support the initiation of condition-directed maintenance; however, it is not yet considered part of a coordinated condition-monitoring program at the plant.

Acoustic Monitoring

Acoustic monitoring is an informal condition-monitoring program in the early stages of development. The program could be developed to assist in the detection of valve leakage and check valve failure. Specific applications of available technology are still being evaluated. As a condition-monitoring program, acoustic monitoring

could help to identify valve performance loss and eliminate unnecessary valve maintenance.

D.8 PLANT INTERVIEWS

In order to collect additional information that could be useful in the PM task selection and identification, interviews were conducted with the plant's maintenance, I&C, ISI, and operations personnel. Each interview lasted an hour or less. The interviews were conducted on a one-on-one basis, and they were purposely informal to create an easy atmosphere for information exchange. Most of the discussion focused on the same list of questions given in Appendix C, Table C-6. The primary goal was to gain additional insight into present maintenance practices, gain knowledge about equipment problems that goes beyond the written records, and identify applicable information that may have ben missed or overlooked.

Significant information obtained as a result of the interviews included:

General Information

- Several condition-monitoring and trending programs are in place. These include oil sample analysis, vibration analysis, the trending of heat exchanger performance data, a motor-operated valve monitoring program, and thermographic monitoring.

- Maintenance personnel receive both on-the-job training and classroom training. Since the cooperating plant is an older plant, maintenance personnel have a great deal of plant-specific experience.

- There is likely little to be gained by further looks at I&C calibration task frequency optimization. Most I&C tasks are done at optimum frequency intervals.

- Instruments that provide input to the process computer are used to calculate thermal heat balance and therefore, are under technical specification requirements.

- Multi-point recorders generally experience a lot of CM shortly after PM work is done.

- Although the FW system motor-operated valves are tested and the packing is inspected under the motor-operated valve monitoring program, there are no maintenance tasks assigned to periodically inspect valve operator lubrication.

- Although the HP heaters are ASME code components, there appears to be no periodic task to verify HP heater relief valve operability.

- Feedwater pump discharge check valves are a noteworthy problem and have numerous failures. Valve design changes have been implemented.

- A significant number of feedwater regulating valve failures are caused by the positioner.

- Although the casing vent vacuum pumps have a high CM load and many failures, they are not important to FW system operation and are only run at Health Physics request.

D.9 RESULTS: COMPARISON OF RECOMMENDATION WITH CURRENT PM PROGRAM

Like the system analyzed in Appendix C, "Demonstration Of Reliability-Focused Maintenance For Standby Components", the Feedwater System (FW) is a safety-related system subject to technical specifications. The effect of proper preventive and corrective maintenance on this system has a direct impact on plant operation and safety. Therefore, the benefits derived from reliability-centered maintenance studies on such systems are quite subtle, and recommended maintenance activity changes are not easily undertaken when changes to technical specification or regulatory commitments are also considered.

From the utility's perspective, the results of the RCM study indicate that, through the application of reliability-centered maintenance, preventive maintenance man-hours can be more efficiently optimized. Several maintenance tasks were identified that were recommended to be deleted, modified, or changed to condition-directed. Three time-directed tasks were recommended to be added. Overall, if the recommendations noted in the RCM study are accepted, the total time-directed preventive maintenance workload on the FW system would be changed from 165 time-directed tasks to 127. The number of condition-directed preventive maintenance tasks would be increased from zero to three. For the purposes of risk-focused maintenance, however, only the three main feedwater pumps were impacted, representing only one type of component task which was recommended to be modified. Only 39 of the original 165 tasks analyzed by the RCM study were related to risk-critical components identified in Appendix B. Table D-5 summarizes the recommendations of the FW RCM study and contrasts these results for the entire system with those which are applicable to identified risk-critical components only.

Most of the components addressed in the following discussions were identified a HIGH or MEDIUM criticality in the RCM study. However, RCM analysis, as shown in Appendix C, Figure C-1, suggests that, even for a highly-critical component, time-directed tasks may not

TABLE D-5

FW SYSTEM RCM RECOMMENDATIONS:
SYSTEM-WIDE AND FOR RISK-CRITICAL COMPONENTS ONLY

	Total Number of Original PM Tasks	Tasks Modified	Tasks Added	Tasks Combined	Tasks Deleted
FW System	165	13 *	3	34	5
FW System Risk-Critical Components Only	39	3	0	0	0

* Three time-directed tasks changed to condition-directed.

always be appropriate. While not specifically quantifiable, following the recommendations is expected to result in lower corrective maintenance activities in the future. (It should be noted that a condition-directed task necessarily requires a time-directed inspection task or some form of monitoring activity to initiate the task. Thus, by monitoring the equipment performance and calling for maintenance when established standards are exceeded instead of initiating maintenance every time-directed performance interval, it may allow one or more intervals to be passed without administrative approval.) More specific discussion regarding the recommended PM program changes is given below.

D.9.1 Heaters

At the plant site, heater maintenance is usually initiated as a result of heater performance monitoring, which is performed monthly as a part of the plant heat balance analysis. Additionally, periodic eddy current testing is done during refueling outages. The unwarranted time-directed teardown and inspection of heaters is inconsistent with RCM goals and is not recommended. Even though the heaters were identified as a high criticality component, no further time-directed maintenance is recommended. (Heaters were not identified as risk-critical components in Appendix A.)

D.9.2 Pumps and Motors

The three main feedwater pumps, which were identified as risk-critical in Appendix A, and the feedwater pump lube oil system were both identified as high criticality components in the RCM study, although the CM activity on these components is extremely low. All time-directed tasks and condition-monitoring tasks performed on the feedwater pumps are recommended to be retained. It should be

noted, however, that lube oil sample analysis results are not presently trended. In order for a lube oil sample analysis program to be of maximum benefit, analysis results should be trended to indicate and identify slowly-developing problems.

The feedwater pump motor and cables are hypotted once per refueling outage. This practice is not recommended on older motors and could lead to accelerated insulation deterioration. More useful information about insulation values can be obtained through polar indexing, especially if polar index values are trended over time. The performance of polar indexing and trending of insulation values is recommended in place of a task to hypot the feed pump motor and cables.

The two casing vent vacuum pumps were identified as medium criticality components in the RCM study. This was primarily due to the fact that these pumps have experienced a high number of failures and are subject to a high level of CM activity. The casing vent vacuum pumps are not critical to the operation of the FW system, and the performance of time-directed maintenance on these pumps would not be cost effective and is not recommended.

The two zinc injection pumps were also identified as medium criticality components in the RCM study. These pumps have also experienced a high level of CM activity, primarily due to zinc sediment clogging the pump or associated valves. A design change is being considered that should reduce the CM load on these pumps. These two pumps are not critical to the operation of the FW system. The performance of time-directed maintenance on these pumps would not be cost effective and is not recommended.

Finally, the three feedwater pump motor-operated lube oil pumps were identified as medium criticality components in the RCM study. These pumps have experienced no failures and have had little or no CM. The performance of time-directed maintenance on these pumps would not be cost effective and is not recommended.

D.9.3 Motor-Operated Valves

The three parallel block valves to the feedwater regulating valves are presently monitored through the motor-operated valve monitoring program. This testing is recommended to be retained.

Most motor-operated valves at the plant site are also meggered and the valve operators are inspected and lubrication checked. Over the past few years, the block valves have not received this maintenance; however, discussions with maintenance personnel indicate this maintenance will be performed at the next refueling outage. Discussion with plant maintenance personnel, previous RCM study results, and input by industry maintenance experts support the contention that meggering is of little value except when

installing or modifying equipment. Additionally, meggering does not serve well as a predictive tool. Meggering is not recommended.

The time-directed verification and inspection of lubrication is recommended to be retained. However, other maintenance and inspections are recommended to be initiated only on a condition-directed basis, based upon the motor-operated valve monitoring program test results and system motor-operated valve operability and stroke timing tests.

The block valves to the feedwater regulating valves are subject to a time-directed maintenance task to inspect the valve packing and adjust or replace as required. The requirement for packing adjustment or replacement can be identified through the performance of other maintenance tasks, surveillance tests, and inspections of these valves. It is recommended that this time-directed task be deleted and performed as required through corrective maintenance.

D.9.4 Relief Valves

The two relief valves on the HP heaters were identified as medium criticality components in the RCM study. No preventive maintenance is presently performed on these relief valves. It is recommended that the valves be lift checked and their set points verified.

D.9.5 Check Valves

The three main feedwater pump discharge check valves, which were identified as risk-critical in Appendix B, were identified as medium criticality components in the RCM study. These valves are presently disassembled and inspected on a time-directed basis. Normally, the unwarranted time-directed disassembly of components for inspection purposes is inconsistent with RCM goals and is not recommended; however, these check valves have experienced failures in the past and have incorporated minor design changes and improvement. Until a satisfactory history of successful operation is obtained, the time-directed disassembly and inspection is recommended to be retained.

D.9.6 Air-Operated Valves

The three feedwater regulating valves, identified as being risk-critical for the "Loss of Feedwater" initiator in Appendix B, were identified as high criticality components in the RCM study. The noteworthy failure modes included failures of:

- seals
- valve positioner

- disconnected valve operator and stem
- worn parts

The time-directed maintenance presently performed on these valves addresses these failure modes and is recommended to be retained. A technical manual review found no additional vendor-recommended preventive maintenance.

The three minimum flow recirculation valves were identified as medium criticality components in the RCM study. A review of the CM history found that limit switches out of adjustment were the primary cause for valve malfunction. These valves receive time-directed maintenance to disassemble and inspect and replace or repair worn parts as required. They are also subject to thermographic monitoring prior to refueling outages, and in-service testing to verify valve operability and stroke time.

The unwarranted disassembly and inspection of valves and components is inconsistent with RCM goals and is not recommended. The disassembly and inspection and repair of minimum flow recirculation valves is recommended to be performed on a condition-directed basis, based on the result of thermographic monitoring and valve operability surveillance tests.

D.9.7 Manual Valves

Fourteen manual valves are subject to time-directed maintenance to inspect and lubricate the valve, check packing, and cycle the valve. Although not specifically referenced, this maintenance activity appears to be in response to IE86-61 addressing valve failures at Rancho Seco. Two of the valves are normally locked closed valves and are insignificant to the operation of the FW system. Therefore, the time-directed maintenance task on these valves is recommended to be deleted, and to be performed as required through corrective maintenance.

Several other manual valves have time-directed maintenance to inspect the valve and repack or adjust packing as required. It is recommended that during this inspection, the valve be cycled and lubrication checked as well.

A large number (34) of manual valves (vent valves, drain valves, isolation valves, and equalizing valves) have a time-directed task to inspect the valve and adjust packing or repack as required. These tasks are intended to preclude the possibility of packing leaks during plant operation that, if severe enough, could necessitate an unplanned plant shutdown or high man-rem exposures to repair. It is recommended that these valve inspections be combined into one thorough system walkdown inspection where all FW system drain valves, equalizing valves, and isolation valves can be inspected and packing requirements addressed.

D.9.8 Flanges, Joints, Gaskets, and Seals

The FW system, especially the feedwater pumps, should be inspected for flange, joint, gasket, or seal leaks, similar to valve packing inspections, as a part of normal operations tours, or as a specific mechanical maintenance task. Periodic system-wide inspections are recommended.

D.9.9 Pressure Switches

Several pressure switches were identified through the RCM analysis as being of either high or medium criticality in the RCM study. A review of the FW system PM summary shows that many of the switches identified as critical are not calibrated and have no time-directed maintenance. Six of these pressure switches were identified as risk-critical in Appendix B. Discussions with I&C personnel at the plant have confirmed that these switches are calibrated as a part of the Condensate (CN) System PM activity.

D.9.10 Level Loops

The zinc injection system tank level loop was identified as being of medium criticality in the RCM study. These components are presently not calibrated as a part of the FW system PM activity, even though this tank level loop does provide control signals to the zinc injection pumps. Calibration drift or component failure could result in zinc injection pump damage or failure. Although the zinc injection pumps are not important to the operation of the FW system, it is more cost effective to periodically calibrate the zinc injection system tank level loop rather than risk pump damage or failure.

APPENDIX E

DEMONSTRATION OF RELIABILITY-FOCUSED MAINTENANCE FOR PASSIVE COMPONENTS

E.1 INTRODUCTION

The identification of risk-critical passive components and the decision to include such risk-critical components in a Reliability Focused Maintenance (RFM) program requires a different set of procedures than that for active components. Unless a monitoring program is already in place, passive components' inherent difference is that they rarely "announce" an impending failure. When a pipe leaks, a vessel fractures, or a seal ruptures there is usually very little warning. The types of maintenance practices available are also limited. Pipes are not lubricated, there are no bearings to replace, electrical cables cannot be replaced, and so forth. Thus, there is an inherently different selection process and rationale for the inclusion or exclusion of passive components.

E.1.1 Failures of Passive Components

To place all of the subsequent discussions in context, it is necessary to describe what is meant by a passive component failure. By definition, a passive component's function is to provide a boundary. It may be a pressure boundary (e.g., the main coolant piping), a fluid boundary (e.g., the service water tank), a force boundary (e.g., dampers on turbine blades), or an environment boundary (e.g., cable insulation). The definition of failure used here is that the boundary is no longer intact. Thus, leaking pipes and frayed cables are examples of failed passive components.

E.1.2 Identification Issues for Passive Components

The fundamental issues that must be considered in the identification of risk-critical passive components, and the subsequent decision to include or exclude them from a RFM program, must include the following three concerns. First, the risk of a passive component failure must be considered, both from the standpoint of the frequency of failure as well as the consequences of that component's failure. Also, the effectiveness of maintenance activities must be factored into the decision as to whether or not a passive component is included in a RFM program. If the effect of maintenance is not included in the criteria for including components then it is possible to perform maintenance which has no net increase in the component reliability and, in fact, may decrease the reliability. For example, repeated proof testing of a piping system early in the service life will decrease the piping reliability. Finally, the types of maintenance activities for passive components are more limited than for the active components. Maintenance activities for passive components will be limited in this discussion to inspection, testing,

refurbishment, and replacement. There are no available techniques for decreasing the change in the failure rate that will be considered.

The remainder of this section describes an approach for identifying the risk-critical passive components in a system given that it is a risk-critical system. For this demonstration, illustrative of the expected level of detail but not exhaustive, the Component Cooling Water System (CCWS) at an operating nuclear power plant has been selected. The results of on-going research, such as that for the Nuclear Plant Aging Research (NPAR) (Reference 1) program, are expected to provide additional information pertinent to the selection of aging-critical components and important age-related degradation and failure mechanisms.

E.2 COMPONENT COOLING WATER SYSTEM (CCWS) DESCRIPTION

The CCWS removes heat from all essential components required for normal and emergency shutdown of the plant with the exception of the diesel generators. The heat is rejected into the Service Water System (SWS) through the CCWS heat exchanger. The CCWS also provides cooling to the fuel pool cooling heat exchangers, reactor coolant pumps, control element drive mechanisms, normal air cooling units, and the normal chillers when the nuclear cooling water system is not available. The CCWS is also viewed as another barrier between the reactor coolant system and the environment for radionuclide transport. The escape path, with the CCWS boundary functional, is through the SWS.

There are two identical, independent, closed loop, flow trains in the CCWS. Each flow train includes a heat exchanger, surge tank, pump, chemical addition tank, piping, valves, controls, and instrumentation. Either of the two trains is sufficient to provide the cooling capacity needed to shutdown the reactor system.

If the SWS is unavailable, then the CCWS will eventually fail because there will be no place to reject the heat. Therefore, in considering the CCWS, the SWS, as a support system to CCWS, must also be examined. The SWS removes the heat from the CCWS and the diesel generator cooling water heat exchangers by dissipating the heat into the atmosphere by the spray ponds. The SWS has two redundant spray ponds and two separate, redundant flow trains, one flow train taking suction from, and returning water to each spray pond. Each flow train consists of an SWS pump, piping, valves, controls, and instrumentation. It is capable of supporting 100 percent of the cooling function following the safe shutdown of the reactor following a LOCA.

Each of the major passive components are listed in the next section. The inclusion or exclusion of each component from the RFM list is then discussed.

TABLE E-1

RISK-CRITICAL PASSIVE COMPONENTS FOR RFM

CCWS PASSIVE COMPONENTS	
System:	Material:
Spray ponds	Reinforced concrete
Spray nozzles	Austenitic stainless steel
Sulfuric acid tank	Carbon steel
Hypochlorite tank	Fiberglass reinforced plastic
Piping	
From SWS pumps	Plasite-lined carbon steel
Distribution headers	Austenitic stainless steel
Filtration train	Plasite-lined carbon steel
Chemical additions system	CPVC plastic
SWS PASSIVE COMPONENTS	
System:	Material:
Heat exchangers	Carbon steel
Surge tanks	Carbon steel
Chemical addition tanks	Carbon steel
Piping	Carbon steel *

* Assumed material type, not found in current documentation

E.3 CRITICAL PASSIVE COMPONENTS IN THE CCWS AND SWS

Table E-1 gives the passive systems which are deemed risk-important because they either are part of the system boundary integrity or are potential radionuclide release paths if they fail. There are several material types that must be considered to assess whether each of these components should be included in a RFM program. The first consideration is the failure mechanism.

These components can fail by one of three credible mechanisms: (1) overload, (2) fatigue and fatigue-related crack growth, and (3) environmentally related failures (e.g., corrosion). Recall that only passive components are being considered so that it is assumed that the active components are available. This is a reasonable assumption if the RFM for active components has been successful. Therefore, the passive equipment is not failing as a result of active component failures[1] and these failure mechanisms provide an appropriate list.

Overload failure mechanisms are excluded from consideration at the present time. The reason is that there is no maintenance activity (inspection, testing, or replacement for passive components) that can guard against an overload. The effect of overloads will be re-introduced as a modification to the fatigue and fatigue-related failures at a later time.

For this specific plant and system, environmental failure mechanisms are also excluded because there is a continuous monitoring system. There is a corrosion rack in the SWS that would detect the onset of corrosion so there is no need to include components in a RFM program for this cause. The final failure mechanism, fatigue, is a difficult problem to address because it is time-dependent and non-linear. That is, as fatigue damage accumulates, the rate of damage accumulation increases (i.e., there is an acceleration in the damage). Thus, a component that is initially in an undamaged state, and thus would not be susceptible to fatigue-related failures, would be excluded from a RFM program. However, ten years after it is placed in service, it may have acquired significant damage and should be monitored or replaced (i.e., be included in an RFM program). The inclusion of such failure mechanisms in the decision as to whether or not a component should be included in an RFM program is discussed in the following section.

E.4 DETERMINATION OF RFM COMPONENTS FOR FATIGUE-RELATED FAILURE MECHANISMS

An effective maintenance activity for passive components will be affected by the ability to detect level of damage. In the case of

---

[1] An example would be the breach of a tank by turbine failure and subsequent missile generation.

fatigue failures, this implies a crack size as a measure of damage. Very small cracks cannot be found with high confidence. Several studies have been published that relate the probability of detection, denoted $P_D(a)$, to the crack size, a. A reasonable review of these probabilities is given in Reference E-2. For the moment, it is simply recognized that the probability of detecting a crack is non-linearly proportional to the size of the crack.

For steels, and in fact many metals, it is sufficient to consider only the crack size. For plastics, particularly chlorinated polyvinyl chloride (CPVC) type plastics, the crack size is not sufficient for tracking damage accumulation. This is because the majority of the material's life is taken up with the initiation of cracks, not the growth of cracks. In fact, the growth of cracks is not represented by a monotonically increasing curve of crack growth rate versus crack driving force. Therefore, the algorithm for deciding whether or not a CPVC plastic component is included in the RFM program must be different from the metal algorithm, since much of a CPVC plastic component's life can be taken up with stable crack growth.

To illustrate the method, carbon steel will be examined. After the algorithm for carbon steel is described, it will be shown how it can be modified to address plastic pipe. Finally, a modification to address overload situations is provided.

Because each of the passive components given in Table E-1 is important to risk control, they must be available a significant fraction of time. The decision as to whether or not a specific component is to be included in the RFM program will thus be made in increments of eighteen months, or roughly every refueling. While passive components suffer from the disadvantage that they are costly to replace and difficult to maintain they enjoy an advantage. Because there are indicators of the future time of failure (e.g., cracks or corrosion), if a passive component is included in the RFM program, then it is possible to safely use the passive equipment for longer periods of time. If the component is not in the RFM program, then passive components usually do not "announce" the failure in the sense of an active component. For example, changes in pump RPMs may be an indication of low lubrication levels, while a piping system goes immediately from a pressure-retaining barrier to non-retaining.

To include the component under consideration in the RFM program the number of refueling intervals that have passed since the component was last included in the RFM program must be less than:

$$R_{CM} = 6.4 \times 10^{9} / (N_{total} \times (1 - \Phi) \times a^{0.859} \times \Delta\sigma^{3.719} \times I_R) \qquad (1)$$

where N_{total} is the total number of fatigue cycles expected over the plant life, Φ is the plant capacity factor, a is the current crack length, I_R is the interval between refuelings, and $\Delta\sigma$ is the stress range. For carbon steel, this formulation will require a

TABLE E-2

NUMBER OF REFUELING INTERVALS BETWEEN MAINTENANCE

CARBON STEEL MATERIAL 18 month refueling periods	
STRESS RANGE, $\Delta\sigma$; 1 ksi	
Initial Crack Size	R_{CM}
0.01	35
0.02	19
0.04	10
0.08	5
0.16	3
0.32	1
0.64	Replace or repair

maintenance activity (i.e., inspection) at that time in which the crack length will double. The constants given in Equation (1) are derived from Reference E-3 and carbon steel fatigue properties. The detailed derivation of the equation is given in the attachment to this appendix.

To see the effect of this guideline, examine Table E-2. In this table, for the given assumptions on the crack size and stress range, the corresponding number of refuelings between maintenance is given. For example, if a 0.04 inch crack can be perfectly detected, then the maintenance for that component need only be performed every ten refuelings. On the other hand, if crack detection can only occur for crack lengths greater than 0.64 inch, then it is necessary to inspect more frequently than every refueling.

There are several advantages to this empirical relationship. Those utilities who use very detailed, and usually more costly, inspection methods in order to find lower levels of damage are not required to perform maintenance as frequently. However, safe operation is reasonably assured, since all of the inspection times are based on damage levels doubling, not on the component failure. Finally, the probability of detecting a crack of a given size can be factored into the analysis as demonstrated below.

Figure E-1 gives the details of the probability of detection for a dye penetrant inspection. This is a commonly-used technique for the detection of surface cracks in steels. Table E-3 shows the crack size, R_{CM}, and detection probability given the crack size, P_D. If a weighted average of the R_{CM} period times the refueling interval is calculated, then one can obtain the start-up inspection time. For the particular values of the carbon steel selected, this would be 5.5 years, or at the fourth refueling.

E.5 SUMMARY

Using the methods developed here it is possible to schedule RFM programs for passive components (see Table E-4). Unlike the active risk-critical component list, this RFM passive component list changes with time.

The effect of an overload on the inclusion of components in the RFM list can now be examined. If Equation (5) in the attachment is examined, then the crack size after one cycle of a high load is:

$$a_{overload} = (a^n_{initial} + nC'\Delta\sigma^m)^{(1/n)}$$

where n is equal to (2-m)/2 and $\Delta\sigma$ represents the overload stress range. If $C'\Delta\sigma^m / a^n_{initial}$ is much greater than 1.0, then there is an overload and there could be more than a doubling of the crack size during the scheduled maintenance. To estimate the factor reduction in the R_{cm} parameter divide the value in Table E-2 by $C'\Delta\sigma^m / a^n_{initial}$.

REFERENCES

E-1. US Nuclear Regulatory Commission, Nuclear Plant Aging Research (NPAR) Program Plan, NUREG-1144, July 1985.

E-2. Harris, D.O., Lim, E.Y., and Dedhia, D.D., "Probability of Pipe Fracture in the Primary Coolant Loop of a PWR Plant; Volume 5: Probabilistic Fracture Mechanics Analysis", NUREG/CR-2189, 5, Aug 1981

E-3. Mayfield, M.E., et. al., "Cold Leg Integrity Evaluation", NUREG/CR-1319, Feb 1980

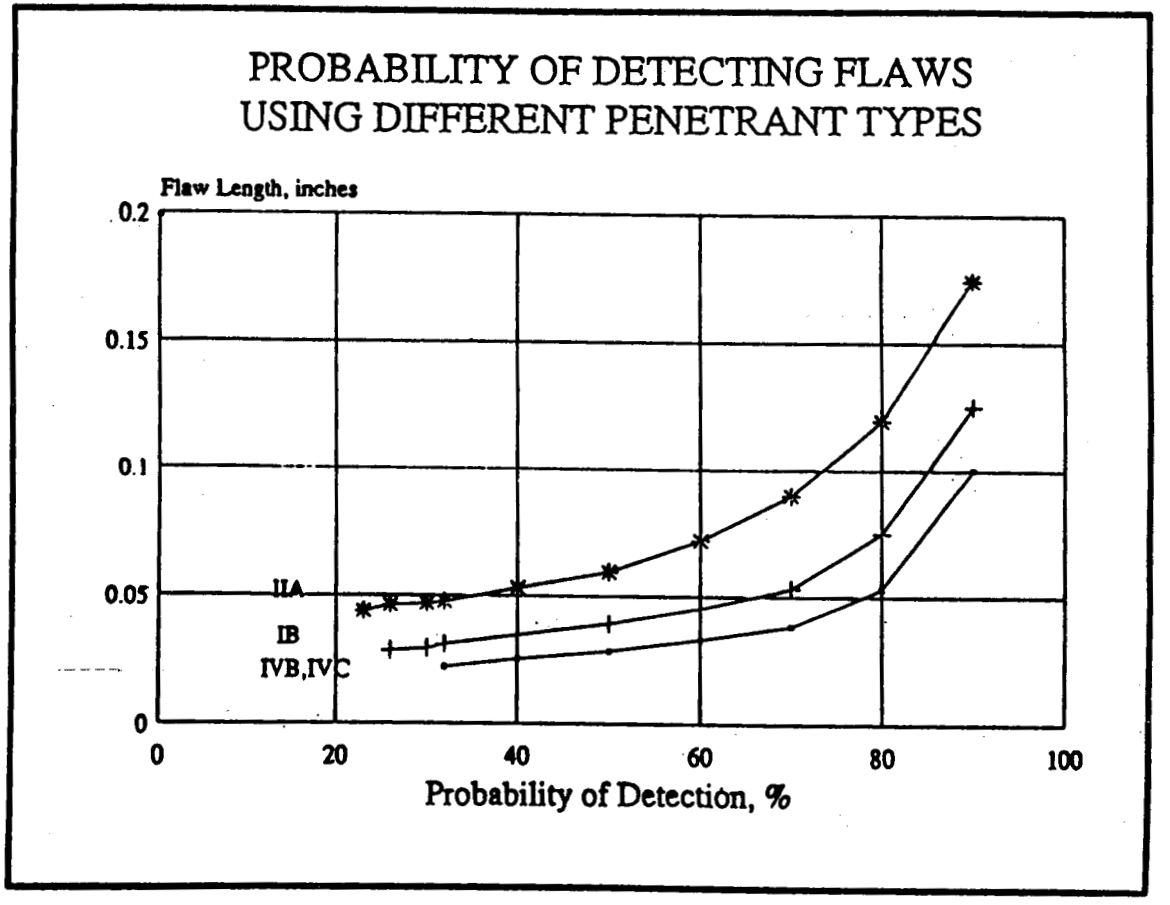


Figure E-1. Detection Probability For Penetrant Inspection

TABLE E-3

AVERAGE INTERVAL FOR INCLUSION IN RFM PROGRAM

FOR CARBON STEEL MATERIAL

Crack Size	$R_{cm}*I_R$ (years)	P_D
0.01	53	10^{-4}
0.02	29	0.01
0.04	16	0.4
0.08	9	0.8
0.16	5	0.9
0.32	3	0.95
0.64	1.5	0.999
$\Sigma P_D R_{CM} I_R / \Sigma P_D$ = 5.5 years		

TABLE E-4

RFM PASSIVE COMPONENT LIST

CCWS PASSIVE COMPONENTS	
System:	RFM Component:
Spray ponds	5th refueling
Spray nozzles	5th refueling
Sulfuric acid tank	See Table E-2
Hypochlorite tank	See Table E-2
Piping	
From SWS pumps	Every refueling
Distribution headers	5th refueling
Filtration train	After corrosion detection in corrosion rack
Chemical additions system	Every refueling
SWS PASSIVE COMPONENTS	
System:	RFM Component:
Heat exchangers	see Table E-2
Surge tanks	see Table E-2
Chemical addition tanks	see Table E-2
Piping	see Table E-2

Attachment to Appendix E

To obtain an expression for the crack size doubling time the crack growth rate equation is examined. In its simplest form it is given as

$$da/dN = C\Delta K^m \tag{1}$$

where

a	crack length
C,m	empirical parameters
K	stress intensity factor
N	number of fatigue cycles at the load level σ.

The stress intensity factor is given as

$$\Delta K = \sqrt{(\pi a)}\Delta\sigma \tag{2}$$

in its simplest form. Normally ΔK is a function of geometry, minimum to maximum stress ratios, and other factors, but for the purposes of this study sufficient detail is provided by the use of equation (2).

It is assumed that the fatigue happens at a constant amplitude and no threshold value is used.* With this assumption, equations (1) and (2) can be combined, resulting in

$$da/dN = C(\sqrt{\pi a})^m \Delta\sigma^m \tag{3}$$

$$a^{-m/2}\, da = C' \Delta\sigma^m\, dN \tag{4}$$

where $C' = \sqrt{\pi^m}$. Integrating equation (4) yields

$$a_f^{(2-m)/2} - a_i^{(2-m)/2} = \frac{2-m}{2} C\pi^{m/2} \Delta\sigma^m \Delta N \tag{5}$$

where a_i is the initial crack size and a_f is the crack size after ΔN fatigue cycles. Using the ASME Section XI "water" line, given in Reference E-3, the doubling time (i.e. that time at which a_f is equal to two times a_i) can be calculated. Setting $a_f = 2a_i$ then results in the following

$$N_{double} = a_i^n(2^n-1)C\pi^{m/2}\, n\, \Delta\sigma^m \tag{6}$$

where $n = (2-m)/2$. Substituting the values from Reference E-3 gives

$$N_{double} = 6.4\times10^9/a^{0.8595}\, \Delta\sigma^{3.719} \tag{7}$$

* The threshold value is the minimum value of ΔK at which crack growth will occur. By not using a threshold value the analysis is conservative.

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC. Add Vol., Supp., Rev., and Addendum Numbers, if any.)
NUREG/CR-5695

2. TITLE AND SUBTITLE
A Process For Risk-Focused Maintenance

3. DATE REPORT PUBLISHED
MONTH: March | YEAR: 1991

4. FIN OR GRANT NUMBER
L1321

5. AUTHOR(S)
E.V. Lofgren, S.E. Cooper, R.E. Kurth, L.B. Phillips

6. TYPE OF REPORT
Technical

7. PERIOD COVERED *(Inclusive Dates)*
Apr. 1990 - Feb. 1991

8. PERFORMING ORGANIZATION – NAME AND ADDRESS *(If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)*

Science Applications International Corporation
1710 Goodridge Drive
McLean, VA 22102

9. SPONSORING ORGANIZATION – NAME AND ADDRESS *(If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)*

Division of Regulatory Applications
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

10. SUPPLEMENTARY NOTES

11. ABSTRACT *(200 words or less)*

This report presents a process for focusing maintenance resources on components that enable nuclear plant systems to perform their essential functions and on components whose failure may initiate challenges to safety systems, so as to have the greatest impact in decreasing risk. The process provides criteria, based on risk, for deciding which components are critical to risk and determining what maintenance activities are required to ensure reliable operation of those "risk-critical" components.

Two approaches are provided for selection of risk-critical components. One approach uses the results of a Probabilistic Risk Assessment (PRA); the other is based on the methodology developed for this report, which has a basis in PRA although it does not use the results of a PRA study. Following identification of risk-critical components, both approaches use a single methodology for determining what maintenance activities are required to ensure reliable operation of the identified components.

The report also provides demonstrations of application of the two approaches to selection of risk-critical components and demonstrations of application of the methodology for determining what maintenance activities are required to an active standby safety system, a normally operating system, and passive components.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

Nuclear power plants
Maintenance
Risk-Focused Maintenance
Reliability-Focused Maintenance Program

13. AVAILABILITY STATEMENT
Unlimited

14. SECURITY CLASSIFICATION
(This Page)
Unclassified
(This Report)
Unclassified

15. NUMBER OF PAGES

16. PRICE

NRC FORM 335 (2-89)

DO NOT MICROFILM
THIS PAGE