RELIABILITY CENTERED MAINTENANCE (RCM) PROGRAM FOR CHASHMA NPP (CHASNUPP)

S. KHALID, S.A. KHAN
CHASNUPP, Chashma Nuclear Power Project,
Islamabad,
Pakistan

Abstract

This paper describes the proposed Reliability Centered Maintenance (RCM) program for Chashma Nuclear Power Plant (CHASNUPP). Major steps are the identification of risk critical components and the implementation of RCM procedures. Identification of risk critical components is based upon the CHASNUPP level 1 PSA results (performed under IAEA TC Project PAK/9/019) which is near completion. The other requirements for implementation of RCM program is the qualitative analysis to be performed for identifying the dominant potential failure modes of each risk critical component and determination of the necessary maintenance activities, required to ensure reliable operation of the identified risk critical components. Implementation of RCM program for these components will lead to improvement in plant availability and safety together with reduction in the maintenance cost. Development / implementation of RCM program at this stage will help the CHASNUPP Maintenance department who is now developing the maintenance program / procedures for CHASNUPP.

1. INTRODUCTION

Chashma Nuclear Power Plant is going to be commissioned in 1999. A level 1 PSA of CHASNUPP is being performed under an IAEA TC project PAK/9/019, first set of the quantification results has been obtained and reviewed. Based upon the first set of quantification results, a list of risk critical components has been developed. This list of risk critical components will serve as the basis for implementation of reliability centered maintenance (RCM) program for CHASNUPP in future. The objective of this paper is to outline a reliability centered maintenance program for CHASNUPP risk critical components, identified from PSA level 1 results.

The selection of these risk critical components is based upon the fact that these enable the plant system to fulfill their essential safety function and the failure of these components may initiate challenges to safety systems. RCM for these components may lead to improvement in plant availability and safety together with reduction in the maintenance cost.

As right now the maintenance program for CHASNUPP is under preparation, this paper helps the Maintenance department to provide a criteria and guidance for establishing a reliability centered maintenance program for the risk critical components that accounts for the unique reliability characteristics of each component.

One major purpose of RCM is to provide a systematic set of criteria, based upon risk, for identifying 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 RCM program.

The proposed RCM program applies to a portion of the total plant maintenance program. Plant equipment receives and should continue to receive maintenance for reasons other than the RCM program described herein. Use of RCM program will not preclude other maintenance activities, the maintenance people considers necessary for proper maintenance of the equipment.

The reliability centered maintenance program, therefore, consists of following two major steps based upon the above description:

1. Identifying risk critical components

2. Determining the necessary maintenance activities, required to ensure reliable operation of the identified risk critical components

The overall process and the first step are "risk focused"; the program for individual components is "reliability focused."

The implementation of the top level program for RCM is illustrated in figure 1-1. The first major step is to determine if the component is critical. If a component is not risk critical, it is not included in the domain of the overall RCM program. If the component is determined to be critical to risk then it is incorporated into a RCM program.

![Diagram of RCM Program Approach](image-url)

**FIGURE 1-1** TOP LEVEL RELIABILITY CENTERED MAINTENANCE (RCM) PROGRAM APPROACH
The process for identifying the risk critical components begins with consideration of the functions that must be performed for safe operation of nuclear power plant. Next step is to 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. Then the support systems for the essential system providing the essential safety function and the components that enable these support systems to provide their support functions are identified. RCM program also identify normally operating systems and components whose failures could initiate an accident or transient which challenges safety. For CHASNUPP since level 1 PSA is near to completion, the above described risk critical component identification process based upon the first set of quantification results, has been completed.

After the identification of risk critical components, RCM program determine what maintenance activities are required to ensure reliable operation of the risk critical components identified. The methodologies evaluate failure modes of the risk critical component identified in the first step and identifies maintenance activities required to defend against those failures and then to be incorporated into a RCM program.

Figure 1-2 illustrates the maintenance evaluation process for risk critical component. RCM methodology is further described in section 3.0.
2. IDENTIFICATION OF RISK-CRITICAL COMPONENTS BASED UPON THE PSA RESULTS

An approach for identifying risk critical component based on using the level 1 PSA result is illustrated in figure 2-1. In order to identify the risk critical component from PSA's accident sequences, the first step is the selection of the core melt frequency that represents the most likely accident scenarios. The next step is to identify the components whose failure modes are represented in this set of accident scenarios. Passive components whose failure would violate the technical specifications success criteria or could result in offsite dose comparable to 10 CFR 100, "Reactor site criteria", would also be designated as risk critical. Determination of risk critical passive components should center on the identification of failure modes that can, or will impact safety. If the failure of a component could initiate an accident or if the component is required to mitigate consequence of any accident, given that it has occurred, it should be considered a risk critical component. Finally any standby component for which aging or common cause failure is a concern, from plant specific experience, should also be added to the list of risk critical component.

In order to identify risk-critical components from accident sequences, only the most likely accident sequences (90% contributors to total CD frequency) 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 failure for each of the "dominant" initiating event are kept as risk critical components.

Another approach that can be used to identify the risk critical component is based upon the importance measures or sensitivity analysis results. However for CHASNUPP the approach based upon the core melt frequency results has been used to identify the risk critical components.

From CHASNUPP PSA level 1 results, the initiating events contributing about 90% to the total core melt frequency are selected as a basis for identifying the risk critical components. For CHASNUPP PSA a list of 27 initiating events have been developed comprising of LOCA’s, transients and support system initiating events. Out of these 27 initiating events, 10 initiating events appeared to contribute 90% to the total core damage frequency, table 2-1 lists these ten initiating events. Table 2-2 lists the systems whose post initiating events failures dominates the analysis results of core melt frequency for these initiating events. The initiating events listed in table 2-1 are selected for identification of risk critical components. From the analysis result of these initiating events, accident sequences contributing about 90% to the core melt frequency are examined for recognition of risk critical components. Table 2-3 represents the risk critical components for CHASNUPP identified from the dominant accident sequences. This list of risk critical components is however preliminary at this stage, as this is based upon the first set of quantification results. There may be slight changes in this list after performing the necessary refinement to PSA model.
CONSIDER ALL CUTSETS THAT CONTRIBUTE TO CORE MELT FREQUENCY FOR ALL ACCIDENT SEQUENCES

SELECT AN APPROPRIATE FRACTION OF CORE MELT FREQUENCY TO BOUND ACCEPTABLE RISK

DETERMINE COMPONENTS WHOSE FAILURES ARE INVOLVED IN ABOVE CUTSETS

DETERMINE COMPONENTS WHOSE FAILURES ARE INVOLVED IN ABOVE CUTSETS

OPTIMAL USE SENSITIVITY ANALYSIS OR IMPORTANCE MEASURES TO VERIFY COMPONENT IMPORTANCE

DETERMINE INITIATING EVENTS INVOLVED IN THE ABOVE CUTSETS

DETERMINE COMPONENTS WHOSE FAILURES WOULD RESULT IN THE ABOVE INITIATING EVENT

ASSESS PASSIVE COMPONENTS AND CONTROL INSTRUMENTS USING NON-PSA METHODS

CRITICAL COMPONENTS LIST

STANDBY OPERATING PASSIVE

FIGURE 2-1 PSA BASED PROCESS FOR RISK CRITICAL COMPONENTS IDENTIFICATION
### Table 2-1 Initiating Events - Dominant to Core Damage

<table>
<thead>
<tr>
<th>NO</th>
<th>Initiating Event</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>L4</td>
<td>Steam Generator Tube Rupture</td>
</tr>
<tr>
<td>2.</td>
<td>T-LOP2</td>
<td>Total Loss of Offsite Power</td>
</tr>
<tr>
<td>3.</td>
<td>T-SMF</td>
<td>Loss of Main Feedwater</td>
</tr>
<tr>
<td>4.</td>
<td>T-SCW</td>
<td>Loss of Component Cooling Water System</td>
</tr>
<tr>
<td>5.</td>
<td>T-CND</td>
<td>Loss of Main Condenser</td>
</tr>
<tr>
<td>6.</td>
<td>T-VWE</td>
<td>Loss of Essential Chilled Water System</td>
</tr>
<tr>
<td>7.</td>
<td>T-EMS1</td>
<td>Loss of 1E 6 KV EMA Power Supply</td>
</tr>
<tr>
<td>8.</td>
<td>T-LOP1</td>
<td>Loss of Offsite Power (220 KV)</td>
</tr>
<tr>
<td>9.</td>
<td>T-GT</td>
<td>General Transients</td>
</tr>
<tr>
<td>10.</td>
<td>L3</td>
<td>Small LOCA</td>
</tr>
</tbody>
</table>

### Table 2-2 Systems - Dominant in Core Damage Accident Sequences

<table>
<thead>
<tr>
<th>NO</th>
<th>System Code</th>
<th>System Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>SAF</td>
<td>Auxiliary Feedwater System</td>
</tr>
<tr>
<td>2.</td>
<td>SRC</td>
<td>Reactor Coolant System</td>
</tr>
<tr>
<td>3.</td>
<td>CRP*</td>
<td>Reactor Protection System</td>
</tr>
<tr>
<td>4.</td>
<td>SAF &amp; VWE</td>
<td>Auxiliary Feedwater System and Essential Chilled Water System</td>
</tr>
<tr>
<td>5.</td>
<td>TG &amp; SAF</td>
<td>Total Grid Loss and Auxiliary Feed Water System</td>
</tr>
</tbody>
</table>

* Note: ATWS are not separately modeled at this stage.

In Table 2-3 the nomenclature used is as follows:

- VBC: Pump Room Ventilation System
- VER-A: 6 KV IE Electrical Building Ventilation System
- SIS: Safety Injection System
- SRH: Residual Heat Removal System
- CES: ESF Actuation System
- VO: Motor Operated Valve
- PO: Motor Driven Pump
- PD: Diesel Driven Pump
- EC/BR: Electrical Breakers
- IND.: Independent Failures
- CCF: Common Cause Failures
<table>
<thead>
<tr>
<th>NO.</th>
<th>SYSTEM</th>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
<th>FAILURE MODES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>SAF</td>
<td>V10A/B/C/D-VO</td>
<td>ISOLATION VALVES</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V12A/BC/D-VO</td>
<td>RECIRCULATION LINES VALVES</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V19A/B-VO</td>
<td>DIESEL DRIVEN PUMP COOLING SIDE</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>P01A/01B-PO</td>
<td>MOTOR DRIVEN PUMPS</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>P02A/02B-PD</td>
<td>DIESEL DRIVEN PUMPS</td>
<td>IND.</td>
</tr>
<tr>
<td>2.</td>
<td>SRC</td>
<td>P01A/01B-BR</td>
<td>SRC PUMP BREAKERS</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TT01A/01B-TT</td>
<td>TEMPERATURE TRANSMITTER</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V02A/02B-VR</td>
<td>PRESSURIZER RELIEF VALVE</td>
<td>IND.</td>
</tr>
<tr>
<td>3.</td>
<td>CRP</td>
<td>QF-EC</td>
<td>BREAKERS</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KD-ER</td>
<td>RELAYS</td>
<td>IND.</td>
</tr>
<tr>
<td>4.</td>
<td>WES</td>
<td>P01A/02A-PO</td>
<td>MOTOR DRIVEN PUMPS</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V07B/08B-VH</td>
<td>PUMP DISCHG. LINE CHECK VALVES</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FT01A-SR</td>
<td>SUCTION STRAINER</td>
<td>IND.</td>
</tr>
<tr>
<td>5.</td>
<td>VWE</td>
<td>101/201-CH</td>
<td>CHILLERS</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>101/201-PO</td>
<td>MOTOR DRIVEN PUMPS</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V207-VH</td>
<td>CHECK VALVE</td>
<td>IND.</td>
</tr>
<tr>
<td>6.</td>
<td>SCW</td>
<td>P02BCD-PO</td>
<td>MOTOR DRIVEN PUMPS</td>
<td>CCF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FT09A/B-WF</td>
<td>WATER FILTER</td>
<td>IND.</td>
</tr>
<tr>
<td>7.</td>
<td>VBC</td>
<td>106/206U-FN</td>
<td>FANS FOR VWE VENTILATION</td>
<td>CCF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V150/250-VO</td>
<td>SRH PUMPS VENT. FAN SUCTION SIDE VALVES</td>
<td>CCF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V266-VO</td>
<td>WES COOLING LINE VALVE</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V169/269-VO</td>
<td>SCW PUMPS VENT. FANS SUCTION SIDE VALVES</td>
<td>CCF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V141/241-VO</td>
<td>SIS PUMPS VENT. FANS SUCTION SIDE VALVES</td>
<td>CCF</td>
</tr>
<tr>
<td>8.</td>
<td>SIS</td>
<td>P01A/B-PO</td>
<td>MOTOR DRIVEN PUMPS</td>
<td>CCF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>P02A/B-PO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>SRH</td>
<td>P01A/B-PO</td>
<td>MOTOR DRIVEN PUMP</td>
<td>CCF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V01A/B-VO</td>
<td>SUCTION SIDE VALVES</td>
<td>CCF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V01C/D-VO</td>
<td>SUCTION SIDE VALVES</td>
<td>CCF</td>
</tr>
<tr>
<td></td>
<td></td>
<td>V09A/B-VO</td>
<td>HEAT EXCHANGER DISCHG. VALVES</td>
<td>CCF</td>
</tr>
<tr>
<td>10.</td>
<td>CES</td>
<td>TRA/B-AR</td>
<td>ACTUATION RELAY</td>
<td>IND.</td>
</tr>
<tr>
<td>11.</td>
<td>VER-A</td>
<td>111FT-WF</td>
<td>WATER RELAY</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HEPA FTA-AF</td>
<td>HEPA FILTER</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SDFTA-AF</td>
<td>SAND FILTER</td>
<td>IND.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HXA-HX</td>
<td>HEAT EXCHANGER</td>
<td>IND.</td>
</tr>
</tbody>
</table>
3. RELIABILITY CENTERED MAINTENANCE PROGRAM METHODOLOGY

This section describes the methodology for developing a reliability centered maintenance program for risk critical components. This methodology is appropriate for establishing a reliability-centered maintenance program for risk critical components identified by the PSA approach described in the preceding sections.

Establishing a reliability centered 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.

Figure 3-1 indicates the two steps that should be addressed by a reliability centered 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 for these dominant failure modes that will be defend against. Methodologies for completing each step are discussed below.

![Figure 3-1](Image)

**FIGURE 3-1 MAINTENANCE EVALUATION PROCESS FOR RISK CRITICAL COMPONENTS**
3.1 IDENTIFICATION OF DOMINANT FAILURE MODES FOR RISK CRITICAL COMPONENTS

Figure 3-2 shows an expanded version of a reliability centered program for identifying the most important component failure modes. Three assessment paths are shown in that figure:

- Identifying the failure modes of the sub-components (elements) of the risk critical components using qualitative, analytical methods
- Identifying failure modes of sub-components (elements) of the risk-critical component 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 components such as diesel generator systems or feedwater systems or where failure history data is not available.

- Assessment Path B would be used for less complex components 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 of sub-components is assumed to be synonymous with identifying the risk critical components. For CHASNUPP right now no risk critical component failure history data is available so RCM program proceeds with the assessment path A. However later on when the plant starts operation and the risk critical components failure history data will be available, assessment path B may also be used.

Assessment path C is compulsory, 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 activities using qualitative, analytical methods to identify dominant failure modes of the risk critical components are characterized by the left most column of figure 3-2. In this option, a qualitative analytical reliability tool such as fault tree, Failure Modes and Effects Analysis (FMEA), or reliability block diagram will be used to identify elements (sub-components) of risk critical components whose failures are of the types:

- Single element (sub-component) failures that fail the component’s function and that are likely to occur

- Latent element (sub-component) that are not detectable through ordinary component demand testing

- Element (sub-component) failures that, though internally redundant, have common cause potential

- Element (sub-component) failures that have large consequences in terms of repair resources required, or that could cascade to more serious failures. The element failures that will be defended against by preventative maintenance or by other means should be chosen from this set.

A failure history assessment option for determining dominant failure modes of the risk critical components is characterized by the box representing assessment path B of figure 3-2. Though at present this option is not being used for CHASNUPP, a brief description about this assessment process is outlined here.

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 appropriate option would be to combine the failure histories of components.
of the same type in the same environment, such as large motor operated valves that see borated water environments. Thus, the first step in this option will be 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 will be to construct a list of failure modes found in the particular data. This should be accomplished in terms of sub-component failures using, if available, sub-component failure cause data. If sub-component failure cause data is not available, the list should be constructed by major sub-component failures (e.g. "valve driver," valve gate binding", etc.).

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

3.2 IDENTIFICATION OF EFFECTIVE MAINTENANCE ACTIVITIES FOR RISK CRITICAL COMPONENTS

The steps to assess existing maintenance requirements and recommendations for each risk critical components are characterized by the box representing assessment path C in Figure 3-2. This assessment will be conducted after, or in parallel with, the assessment in path A or B; it is not considered an option.

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

Reasoning will be defined for both sets of maintenance actions. That is, a basis will be developed for each maintenance action that is included in the existing maintenance plan, and a basis will be developed to explain why each recommended performance is in the 'not performed' category. This explicit set of steps will 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.

The process of determining effective maintenance to defend against the dominant failure modes of a component is mainly based upon the engineering judgment. However, there are some options based upon the information about sub-component's failure mode, its impacts, occurrence frequency and failure type. Such information tables can aid systematic completion of the task of effective maintenance determination. Table 3-1 represents one configuration that may 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 sub-component failures. Succeeding columns, from left to right, list:

- Consequences of these sub-component failures in terms of resources for repair, impacts on risk, impacts on technical specifications (if any), potential for cascading or common cause failure, etc.
<table>
<thead>
<tr>
<th>CRITICAL FAILURE MODE</th>
<th>FAILURE MODE IMPACTS</th>
<th>OCCURRENCE FREQUENCY</th>
<th>INSTRUMENTATION</th>
<th>LATENT OR ANNOUNCED</th>
<th>POTENTIAL DETECTION OR DEFENSE</th>
<th>CRITICAL FAILURE MODES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• The estimated occurrences frequency for each sub-component 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 sub-component has failed or is likely to fail.

• Whether the sub-component failure is latent or announced.

• Potential maintenance defenses such as preventive or predictive maintenance, surveillance, etc. that could be used to detect the sub-component failure or a precursor to sub-component failure or prevent failure.

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

REFERENCES


3. Reliability & Maintainability in Perspective by David J.Smith