RELIABILITY ASSURANCE PROGRAM PLAN

FOR THE

SYSTEM 80+ NUCLEAR POWER PLANT

JANUARY 1992
Rev. 00

ABB COMBUSTION ENGINEERING NUCLEAR POWER
WINDSOR, CONNECTICUT

DRAFT

ABB
ASEA BROWN BOVERI

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ACRONYMS

ALWR	Advanced Light Water Reactor
CFR	Code of Federal Regulations
COL	Combined Operating License
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute
FMEA	Failure Modes and Effects Analysis
FOAKE	First Of A Kind Engineering
KAG	Key assumptions and Groundrules
LCO	Limited Condition of Operation
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Analysis
RAMI	Reliability, Availability, Maintainability, and Inspectability
RAP	Reliability Assurance Program
RIG	Risk Based Inspection Guide
R-Y	Reactor Year
SAMP	Severe Accident Management Procedures
SAR	Safety Analysis Report
SRP	Standard Review Plan
T/S	Technical Specification

RELIABILITY ASSURANCE PLAN
FOR THE
SYSTEM 80+ NUCLEAR POWER PLANT

1.0 INTRODUCTION

1.1 Purpose

System 80+ is a standard nuclear power plant design that is to be certified under 10CFR Part 52[1]. As such, a Level III Probabilistic Risk Assessment (PRA) has been prepared at the onset of the design and licensing processes, and will be updated during the subsequent engineering, procurement, and construction processes. This PRA will be maintained and updated as the design details increase, and will be delivered to the owner/operator upon completion of plant startup. The owner/operator will either maintain the PRA themselves or have the PRA maintained by another organization as a living document that reflects the operating plant as it evolves.

The Reliability Assurance Program (RAP) defines a program for maintaining consistency between the System 80+ PRA and the Plant configuration. The program will ensure that the Procedures and Technical Specifications and plant configuration (including maintenance) are consistent with the PRA. The program defined herein is intended to cover the entire life-cycle of a System 80+ Standard Design Nuclear Power Plant. This plan may be modified by the holder of the Combined Operating License (COL) to contain plant specific information. The RAP is specified as part of the EPRI ALWR Utility Requirements[2].

1.2 Scope

The RAP describes the elements of the program for maintaining the PRA, and conducting a Reliability, Availability, Maintainability, and Inspectability (RAMI) program, and a Reliability Centered Maintenance (RCM) program for the entire plant (both the NSSS and BOP) covered by the certification. It assures consistency between the PRA bases and the plant operation, maintenance and configuration. The RAP plan will be updated and expanded as appropriate as the design moves through certification, First Of A Kind Engineering (FOAKE) and plant specific engineering. Further updates to the RAP will be included in this report as the project progressed through procurement, construction, and operation.

The RAP describes the interface of the PRA with the plants Operating Procedures, Emergency Operating Procedures, Severe Accident Management Procedures, Test and Maintenance Procedures, Technical Specifications and security.

2.0 PRA PROGRAM ELEMENTS

The RAP program includes the elements that are necessary to ensure that the PRA is maintained consistent with the plant configuration and operation. This requires a living PRA that reflects the plant as it progresses from design and construction, and through the operation phase. Therefore the PRA program will be integrated with the other aspects of the plant life cycle. The living PRA is being integrated with the design, operation procedures, maintenance procedures, emergency procedures, and general management of the plant.

2.1 PRA Goals

The RAP assures that the bases of the PRA remain valid and that the plant continues to meet the ALWR reliability and safety objectives. The safety objectives for the ALWR is to have an individual early mortality risk of less than $5x10^{-7}$/R-Y and a cancer mortality risk of less than $2x10^{-6}$/R-Y. This implies a large release potential for offsite early fatalities of less than $1x10^{-6}$/R-Y. The core damage frequency for ALWRs is to be less that $1x10^{-5}$/R-Y.

2.1.2 PRA Methodology

Standard methods were used by ABB-Combustion Engineering in the performance of the System 80+ PRA[4]. The level 1 (core damage frequency) portion of the analysis is equivalent to the baseline probabilistic safety analysis (PSA) described in the PSA Procedures Guide[5] and the methods employed were consistent with methods outlined in the PSA Procedures Guide and methodologies described in the PRA Procedures Guide[6]. The methods used in the PRA were also in conformance with the recommendations of the "PRA Key Assumptions and Groundrules" in Appendix A to Chapter 1 of the EPRI ALWR Requirements Document[7]. The small event tree/large fault tree approach is used for the evaluation of core damage frequency.

External events are defined as those events that result in a plant perturbation or transient, but are not initiated by the plant systems. External events were identified by reviewing past PRAs[8 thru 15] and PRA guidance documents such as the PRA Procedures guide[6], the PRA Fundamentals document[16] prepared by BNL, and the ANS guide for selecting external events[17]. Events with similar plant effects and consequences were grouped together. Criteria were established to determine which external events are insignificant risk contributors and thus can be excluded from detailed quantitative evaluation. The screening criteria was based on design requirements set forth in the EPRI ALWR Utility Requirements Document[7], generally accepted regulatory practices as documented in the NRC Standard Review Plan (SRP)[18] considerations, and generic siting considerations. Each external event identified was then evaluated against the screening criteria to determine whether detailed quantitative analysis is needed. This evaluation also considered the insights gained from a review of PRAs for present generation power plants[9 thru 15].

The methods used for the level 2 severe accident progression, containment response and source term analyses were consistent with the methods used in NUREG-1150[8], the methods described in the PRA Procedures Guide[6] and those methods recommended in the EPRI ALWR Requirements Document[7]. The level 3 analyses

(consequences) also use methods consistent with those described in the PRA Procedures Guide[6] and the methods recommended in the EPRI ALWR Requirements Document[7]. Figure 2-1 shows the major PRA tasks.

All three levels of the PRA require a bases of the plant configuration, equipment mean time between failure (MTBF), mean time to repair (MTTR), inspection intervals, operator procedures, and other aspects of the plant operation. These bases are given in the report "Analysis Assumptions for the System 80+ Standard Design Probabilistic Risk Assessment[3]". This document is an integral part of the living PRA and is updated as needed.

2.3 PRA During Design and Construction

This full-scope PRA program has been conducted using a representative site. Event tree and fault tree models were developed for the design. These models were integrated and used to estimate the feasibility of meeting the plant risk and core damage frequency goals and to provide insight into design decisions. A component reliability data base and component naming convention were established. A baseline level 1 PRA model was developed.

In the second phase, the scope of the PRA was extended to provide detailed models of the support systems, to include a detailed containment analysis and to calculate consequences in terms of off-site doses. This phase identified the dominant core damage contributors and the dominant contributors to off-site releases. The models were used to determine the impact of design changes on core damage and on large release frequency and to identify the dominant contributors. This information was be fed back to the system designers for consideration in the design.

The third phase, following Design Certification by the U.S. NRC, will involve a continuation of the interactive reliability assurance process in which, the PRA practitioners participate during the FOAKE phase. The system fault tree models developed in earlier phases will be modified to evaluate and reflect proposed system design enhancements and details and the engineers with system design responsibility, will be continually appraised of the reliability of their systems vis-a-vis achievement of the plant risk objectives.

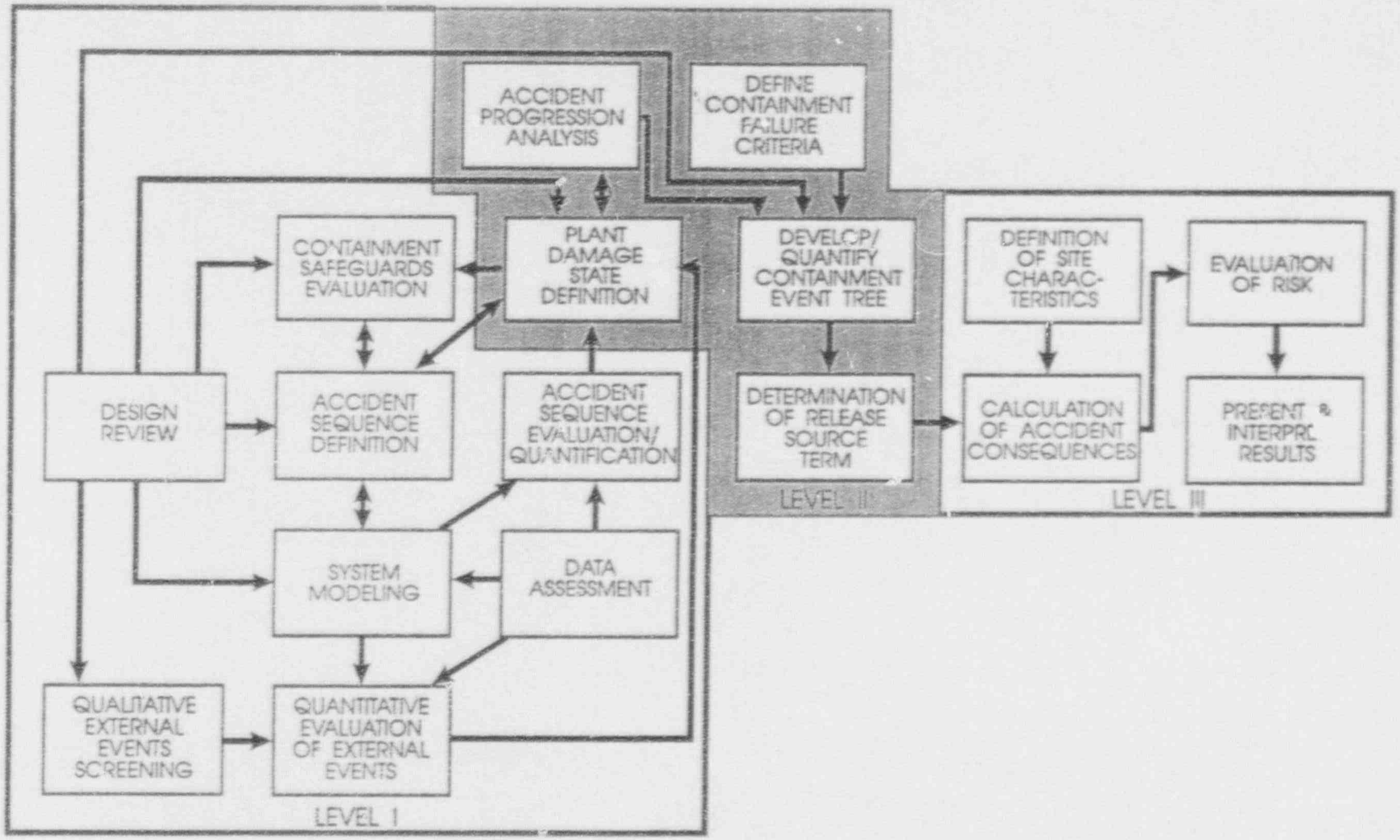
During the procurement and construction phase, the PRA will be maintained current to reflect the "as built" and site specific design and procedures. The PRA will be delivered to the owner/operator after completion of construction and startup.

2.4 PRA During Operation

The PRA will be installed on a computer and delivered for use at the Utility. Appropriate training and documentation will be provided so that the Utility Engineering staff will be able to maintain the PRA current over the life of the plant, and to use the PRA as input to operations and maintenance decisions. The Utility Staff will maintain the PRA using procedures to be developed by the Utility. The PRA will be used to evaluate potential design changes. System fault trees will also be used in the RAMI Program and to support the Reliability

Figure 2-1

MAJOR PRA TASKS



Centered Maintenance Program. The PRA will be updated at regular intervals with plant specific data collected in the Plant Reliability Data Base (part of the RAMI program). In addition, The PRA will be used to support the Significant Event Evaluation Program by using the PRA to evaluate plant events as precursors to core damage sequences. Updated system fault trees will also be used to track the Technical Specifications and LCO conditions by tracking the dependencies of equipment and systems.

3.0 RAMI PROGRAM ELEMENTS

The RAMI Program will be developed by Combustion Engineering to predict and track plant availability in the same way that the PRA follows plant risk. The RAMI Program will be conducted within the context of a RAP Program. The PRA and RAMI efforts use data, methods and analyses which are similar and complementary. After plant startup, the utility will maintain the RAMI Program and ensure that it is consistent with the plant configuration, procedures, and operating history.

3.1 RAMI Analysis

In the design process, reliability engineers sub-divide the top level quantitative Capacity Factor requirements into system level quantitative design requirements. These quantitative requirements will be addressed by each system design engineer. As the system designs evolve, the reliability engineers perform Failure Modes and Effects Analyses (FMEAs) and perform fault tree analyses for systems determined to be important to the plant's ability to meet its quantitative requirements. Standard methods will be used in the performance of the System 80+ RAMI fault trees. The RAMI modeling will be performed in manner much like the Level I (core damage frequency) portion of the analysis described in the PSA Procedures Guide(5) and the methods employed are consistent with methods described in the PRA Procedures Guide(6). The results of these analyses are provided to the design engineers to confirm that their designs meet quantitative requirements and identify which specific design characteristics are limiting. As the design progresses, the system level and component level quantitative reliability requirements will be established to assure that top level requirements are met cost effectively. Through this iterative process, communication is maintained between system designers and reliability engineers.

The central features of the RAMI program are:

1. Reliability Analysis - Failure Modes and Effects Analysis are used to evaluate the potential impacts of component malfunctions on plant operability.

2. PRA Methodology - Fault Tree Analysis methods are used to probabilistically predict and quantify plant availability and plant capacity factor.

3. Design Review - A formal design review procedure is implemented to provide a vehicle for assuring that communication is maintained between the system designers and the engineers performing the RAMI analyses.

The component failure rate data base, for use in the fault tree analyses, will be updated during the FOAKE phase, with generic data chosen at the beginning and being replaced with design specific data as it becomes available. This revised data base will become part of the PRA data base and integrated into the Plant Reliability Data Base (see Section 3.2).

The Design Review Meetings will provide the forum for system designers, reliability engineers and project management to discuss RAMI consideration and

[illegible]ies. Items that are being specifically addressed in the sy[illegible]lyses and in interactions between reliability engineers and syst[illegible]include:

1) Identification of component failures, combinations of component failures, test and maintenance errors, and operator errors that can lead directly, or through the technical specifications, to an outage or reduced production,

2) Identification of Critical Components;

3) Identification of Dominant causes of outages,

4) Identification of each system's status with regard to meeting the RAMI quantitative goals.

The RAMI Analyses will be maintained current with the design as design details become available during the construction and start-up of the plant. In addition, the final RAMI Model will be installed on a computer and delivered for use at the Utility. Appropriate training and documentation will be provided so that the Utility Engineering staff will be able to maintain the RAMI models current over the life of the plant, and to use the RAMI models as input to operations and maintenance decisions.

3.2 Plant Reliability Data Base

Both the PRA, RAMI, and RCM programs need an integrated data base. The Plant Reliability Data Base started out as the PRA data base. The PRA data base is also used for the initial RAMI models. This data base is expanded to include plant specific data as it is accumulated. This insures that the Living PRA, RAMI, and the RCM programs use consistent data. It enables an easy comparison of generic data and plant specific data.

A PRA data base was developed during the design phase and will be expanded during the procurement and construction phases. PRA data is needed for the quantification of the system fault trees and the system accident sequences which result in severe core damage. The data needed for this quantification includes:

A. Initiating event frequencies,
B. Component failure rates (demand and time-dependent),
C. Component repair times and maintenance frequencies,
D. Common cause failure rates,
E. Human failure probabilities,
F. Special event probabilities (e.g. restoration of offsite power),
G. Error factors for the items above.

Generic reliability data are being used appropriately per the guidance in the PSA Procedures Guide[5]. The primary source of data used for the PRA in the Preliminary Design Phase are the "PRA Key Assumptions and Groundrules" (KAG) document (Appendix A to Chapter 1 of the EPRI ALWR Requirements Document[7]).

other industry-accepted generic data sources will be used as needed to supplement the data in the KAG.

The Plant Reliability Data Base will contain both the generic PRA data and plant specific data on the same items. This will enable a comparison of the data, and upgrading of the PRA and RAMI analysis. Dates of maintenance requests will be stored so that Aging Analysis can be performed. The plant Reliability Data Base will be consistent with the NPRDS, a nuclear component data base maintained by INPO.

3.3 Corrective Actions Program

Part of the RAP program is the Corrective Actions Program. This program has been placed as part of the RAMI section because the most common corrective actions will deal with availability improvements with both the nuclear island and balance of plant. The Utility will develop a Corrective Actions Group that will review suggested plant changes to ensure that they are consistent with safety and plant availability goals. The Corrective Actions Group will also review all reactor trips, NRC SER Reports and reported events at other sites that could have significant availability or safety implications. The Corrective Actions program will involve senior representatives from Plant Management, Operations, Maintenance, PRA, and the RAMI groups. Its chairman will report directly to the Plant Manager. Details of the group composition and procedures will be described in this section of the RAP at a later time. Its organizational interfaces are given in Section 6.

4.0 RELIABILITY CENTERED MAINTENANCE PLAN

The PRA incorporates the mean time between failures, mean time to repair, and inspection intervals on the equipment that support plant safety. These equipment characteristics are strongly affected by the maintenance program. Reliability Centered Maintenance (RCM) is a structured, programmatic approach to determine how to prudently and economically maintain plant equipment. RCM embodies the attributes of reliability, availability, maintainability and inspectability. An RCM program will be developed during the plant specific design phase of the System 80+ development with sufficient breadth and detail to support operational decisions.

4.1 RCM Phases

The detailed RCM Program Guide will be developed during the Plant Specific design phase and either included here or referenced in this document. The RCM program will be integrated with the PRA program. The PRA group will supply to the maintenance planning group the MTTR, MTBF and inspection intervals used in the PRA. They will also supply to the RCM group the major sequences leading to core damage and an evaluation of the importance of each system in terms of plant risk reduction. The maintenance planning group will review the PRA bases and ensure that it is included into the RCM program. Discrepancies between the PRA and RCM programs will be eliminated in an iterative fashion. The various phases of the RCM program are outlined below.

Initiation Phase:

This phase involves developing and organizing the following information:

1) Description of system function for each operating mode. Description of component functions for all components within the system which can affect the system function.
2) Descriptions of how the system and its components perform their intended functions.
3) Descriptions of performance tasks which are required to enable the system and its components to continue to perform their intended functions.
4) Description of the PRA and RAMI models for each system including equipment data.
5) Develop Risk-based Inspection Guides (RIGs) based on the PRA and other available guidance.

Implementation Phase:

This phase includes developing:

1) Specific descriptions on how to perform each of the performance tasks.
2) Identification of the resources required to accomplish each of the performance tasks.
3) Descriptions of the scheduling process for each of the performance tasks.

Testing Phase:

This phase in which the RCM Program is tested involves:

1) Identification of functional reliability factors currently being produced by the system and its components.
2) Descriptions of the differences between the actual system reliabilities and intended reliabilities.
3) Identification of the Effectiveness Coefficients of the maintenance program for the system and its components.

Evaluation Phase:

This phase involves:

1) Identification of the causes for the differences between the actual system reliabilities and the intended reliabilities.
2) Descriptions of the changes in the performance of tasks which need to be made in order to reduce the differences between the actual system reliability and the intended reliabilities.
3) Descriptions of any changes which need to be made to the system or the system reliability model in order to make the ideal reliability goals more practically achievable.
4) Review the age related characteristic of all components for wearout.
5) Review the cost-effectiveness of current maintenance procedures.
6) Review the maintenance requirements for evolutionary trends.
7) Review for consistency with the PRA and RAMI programs.

5.0 PROCEDURES AND TECHNICAL SPECIFICATIONS

Imbedded in the System 80+ PRA are requirements dealing with the availability of equipment, and their inspection and maintenance frequencies. The PRA also contains assumptions about operator actions during transients and additional recovery actions that an operator will take after system failures or during an accident sequence. The RAP Plan ensures that the bases used in the PRA are consistent with the plant procedures and Technical Specifications.

5.1 Technical Specification

The Plant Technical Specifications (T/S) describes the operating envelope for the plant. It specifies what equipment must be available and how long the plant can operate with a piece of safety related equipment out of service. Surveillance requirements and frequencies are also specified. The operating conditions in terms of temperatures, pressures and fluid levels are specified in the T/S to ensure that they are bounded by the safety analysis presented in the SAR. The validity of the PRA is also dependent on plant operating limits as specified in the T/S. The PRA group will supply to the procedures group the initial system descriptions from the PRA for review by the procedures group. All proposed or actual T/S changes will be transmitted by the procedures group to the PRA group to be evaluated in the living PRA. The Plant Manager will be notified of any T/S changes that adversely effect the plant risk with respect to the safety goals.

If the Utility chooses to use a computerized T/S monitoring system, the PRA group is responsible to maintain the system fault trees used in the monitoring system. This is to ensure that the T/S models are consistent with the plant configuration and PRA models.

5.2 Plant Operating Procedures

Consistency between the Plant Operating Procedures and the PRA will be maintained. The operations group will be given system descriptions from the PRA for their review and comment. Changes in the operating procedures will be transmitted to the PRA group to be incorporated in the living PRA. The PRA group will perform a special review of all shutdown procedures for their effect on shutdown risk. The Plant Manager will be notified of procedural changes that adversely effect the plant risk with respect to the safety goals.

5.3 Emergency Operating Procedures

The Emergency Operating Procedures (EOPs) describe the operator actions during transients and off normal events. It is important that there is consistency between the PRA and the EOPs as both evolve during the plant life. The PRA contains assumptions about operator actions for all transients. The procedures group will be given system and transient descriptions from the PRA for their review and comment. They will also be given the dominant (most probable) sequences and equipment failures so that they can ensure that the EOPs reflect the most probable accident sequences. Changes in the EOPs will be transmitted to the PRA group to be incorporated in the living PRA. The Plant Manager will

be notified of EOP changes that adversely effect the plant risk with respect to the safety goals.

5.4 Severe Accident Management Procedures

The Severe Accident Management Procedures (SAMPs) are to provide the Plant with a framework for evaluating information on severe accidents, and ensure effective response to credible severe accidents. They will most likely be extensions of the EOPs and will guide the operator to maintain the safety functions and safety goals within the context of the EOPs. The SAMPs require the evaluation of phenomenological behavior of core and structural material beyond design base conditions. Both equipment and instrument performance in severe environments must be evaluated for the selection of strategies to mitigate consequences of the accident. The Severe Accident Management Procedures (SAMPs) give operators guidance during events beyond design bases. It is important that there is consistency between the PRA and the SAMPs as both evolve during the plant life. The PRA contains assumptions on operator actions for all transients and include recovery actions after systems fail and recovery actions during accident sequences. The procedures group will be given system and transient descriptions and potential recovery actions from the PRA for their review, comment, and inclusion in the procedures. They will also be given the a description of the most probable sequences and equipment failures predicted in the PRA so that they can ensure that the SAMPs reflect the most probable accident sequences. Changes in the SAMPs will be transmitted to the PRA group to be incorporated in the living PRA. The Plant Manager will be notified of SAMP changes that adversely effect the plant risk with respect to the safety goals.

5.5 Security

The PRA identifies the most likely (in terms of frequency) sequences that lead to core damage and the importance of each system in preventing or mitigating core damage and large releases. This "road map" is important to plant safety. Plant Security will be given a summery of the importance of each system in preventing accidents and the dominant (most likely) sequences that accidents might follow. This information is important to the prevention of sabotage and in emergency preparedness planning.

6.0 ORGANIZATIONAL AND ADMINISTRATIVE SUPPORT

This section will contain the organization charts for the Utility, plant Staff and Designers who support the RAP program when such information becomes available.

7.0 REFERENCES

1. 10 CFR Part 52; Early Site Permits: Standard Design Certification and Combined Licenses for Nuclear Power Reactors; 54FR 15372; April 18,1989.

2. EPRI, Advanced Light Water Reactor Utility Requirements Document, Vol. III, Chapter 1: Overall Requirements, Paragraph 6.2.1.1, Reliability Program, August 31, 1990.

3. "Analysis Assumptions for the System 80+ Standard Design Probabilistic Risk Assessment", ABB Combustion Engineering Nuclear Power, DCTR-RS-03 Rev.0, May 1991.

4. Base Line Level 1 Probabilistic Risk Assessment for the System 80 NSSS Design; Enclosure (1)-p to LD-88-008; Combustion Engineering, Inc.; January,1988.

5. NUREG/CR-2815; Probabilistic Safety Analysis Procedures Guide; Papazoglou, I. A., Bari, R. A.; Brookhaven National Lab.; January 1984.

6. NUREG/CR-2300; PRA Procedures Guide; April 1982.

7. Advanced Light Water Reactor Utility Requirements Document, EPRI, Draft, April, 1987.

8. NUREG-1150; Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plants, Second Draft for Peer Review; U. S. Nuclear Regulatory Commission; June, 1989.

9. Zion Probabilistic Safety Study, Commonwealth Edison.

10. Oconee PRA: A Probabilistic Risk Assessment of Oconee Unit 3, NSAC/60, June 1984.

11. Seabrook Station Probabilistic Safety Assessment, PLG-0365; Prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company; Pickard, Lowe and Garrick, Inc., June, 1984.

12. Indian Point 2 and 3 Probabilistic Safety Study; prepared for Consolidated Edison Company of New York, Inc., and Power Authority of the State of New York; Pickard, Lowe, and Garrick, Inc.; March, 1982.

13. Savannah River Site Probabilistic Risk Assessment of Reactor Operation, Draft by the Westinghouse Savannah River Company, August 31, 1989.

14. NUREG/CR-4840; Procedures for the External Event Core Damage Frequency Analyses for NUREG-1150; Bohn, M. P., Lambright, J. A.; prepared for the U.S. Nuclear Regulatory Commission by Sandia National Laboratories; November, 1990.

15. NUREG/CR-4550, Vol. 3, Rev. 1, Part 3; Analysis of Core Damage Frequency: Surry Power Station, Unit 1 External Events; Bohn, M. P. et. al.; prepared

for the U. S. Nuclear Regulatory Commission by Sandia National Laboratories; December, 1990

16. Probabilistic Risk Assessment: Fundamentals; prepared by Brookhaven National Laboratory, prepared for the U.S. Nuclear Regulatory Commission; Fullwood, R. R.; March, 1987.

17. American Nuclear Society; Guidelines for Combining Natural and External Man-Made Hazards at Power Reactor Sites; ANSI/ANS-2.12-1978.

18. NUREG-0800; Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, LWR Edition; U.S. Regulatory Commission; July, 1981.