IAEA-TECDOC-1264

# *Reliability assurance programme guidebook for advanced light water reactors*

INTERNATIONAL ATOMIC ENERGY AGENCY

December 2001

The originating Section of this publication in the IAEA was:

Nuclear Power Technology Development Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

RELIABILITY ASSURANCE PROGRAMME GUIDEBOOK FOR
ADVANCED LIGHT WATER REACTORS
IAEA, VIENNA, 2001
IAEA-TECDOC-1264
ISSN 1011–4289

Printed by the IAEA in Austria
December 2001

# FOREWORD

To facilitate the implementation of reliability assurance programmes (RAP) within future advanced reactor programmes and to ensure that the next generation of commercial nuclear reactors achieves the very high levels of safety, reliability and economy which are expected of them, in 1996, the International Atomic Energy Agency (IAEA) established a task to develop a guidebook for reliability assurance programmes. The draft RAP guidebook was prepared by an expert consultant and was reviewed/modified at an Advisory Group meeting (7–10 April 1997) and at a consults meeting (7–10 October 1997). The programme for the RAP guidebook was reported to and guided by the Technical Working Group on Advanced Technologies for Light Water Reactors (TWG-LWR).

This guidebook will demonstrate how the designers and operators of future commercial nuclear plants can exploit the risk, reliability and availability engineering methods and techniques developed over the past two decades to augment existing design and operational nuclear plant decision-making capabilities.

This guidebook is intended to provide the necessary understanding, insights and examples of RAP management systems and processes from which a future user can derive his own plant specific reliability assurance programmes. The RAP guidebook is intended to augment, not replace, specific reliability assurance requirements defined by the utility requirements documents and by individual nuclear steam supply system (NSSS) designers.

This guidebook draws from utility experience gained during implementation of reliability and availability improvement and risk based management programmes to provide both written and diagrammatic “how to” guidance which can be followed to assure conformance with the specific requirements outlined by utility requirements documents and in the development of a practical and effective plant specific RAP in any IAEA Member State.

The IAEA wishes to thank all the participants, including N. Hunt who prepared the draft guidebook, for their valuable contributions. The IAEA is particularly grateful to the Government of the Republic of Korea for providing extra-budgetary funds to support this guidebook. The IAEA staff members responsible for this guidebook were Doo-suhk Suh, Byung-oke Cho and Yang-Eun Kim of the Division of Nuclear Power.

## *EDITORIAL NOTE*

*The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.*

*The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.*

## CONTENTS

# 1. INTRODUCTION TO RELIABILITY ASSURANCE

## 1.1. INTRODUCTION

In 1996, the IAEA initiated a task to develop a reliability assurance (RA) guidebook to support the implementation within advanced reactor programmes and to facilitate the next generation of commercial nuclear reactor to achieve a high level of safety, reliability and economy. The guidebook is intended to demonstrate how designers and operators of future commercial nuclear plants can apply the risk, reliability and availability engineering methods and techniques developed over the past two decades to augment their existing design and operational nuclear plant capabilities and design a plant specific reliability assurance programme.

The RA guidebook draws from utility experience gained during past implementation of reliability and availability improvement and risk based management programmes and demonstrates how quantitative and qualitative techniques during each phase of plant life and use reliability assurance methods, techniques and programmes to optimize plant economic performance and safety.

This guidebook is expected to serve as a resource for organizations which are considering the implementation of a reliability assurance programme and demonstrate how reliability assurance methods, techniques and programmes can be used during each phase of plant life to optimize its economic performance and safety, i.e. achieve maximum performance at minimal cost within all superimposed constraints. The techniques available for application in reliability assurance include the well established:

- Reliability, availability and maintainability (RAM) analysis,
- Probabilistic safety assessment (PSA),
- Economic modelling and quantification techniques which allow cost-benefit analysis and optimization of overall economic performance.

The approach to reliability assurance proposed within the guidebook complements the system engineering of the plant design and is consistent with the integrated logistic support (ILS) initiative which has been developed to achieve the best balance between cost, schedule, performance and supportability, i.e. manpower, personnel and skills.

The implementation of a reliability assurance programme provides a structured way of meeting regulatory and utility requirements for the next generation of nuclear power plants.

A RA programme complements the overall safety assessment and uses the PSA as a basis for cost/benefit analysis and optimizing safety processes during the design phase and evaluation modifications to the plant when it is in the operational phase. In addition, an RA programme provides a sound basis for establishing the Technical Specifications. The reliability assurance programme complements the quality assurance programme in that they each have similar objectives, but achieve them in different ways.

Note: Throughout this publication two conventions are used to refer to abbreviations for reliability assurance and the reliability assurance programme. These are equivalent and are as follows:

- RA programme
- RAP

In addition, the following terms should be explained:

- Probabilistic risk assessment (PRA) is equivalent to probabilistic safety assessment (PSA);
- RAM generally refers to reliability, availability and maintainability, whereas RAMI refers specifically to reliability, availability and maintainability improvement.

### 1.1.1. Safety assessment and probabilistic safety assessment (PSA)

Safety assessment (INSAG-3) includes systematic critical review of the ways in which structures, systems and components (SSCs) might fail and identifies the consequences of such failures. The assessment is undertaken expressly to reveal any underlying design weaknesses. Two complementary methods, deterministic and probabilistic, are currently in use to jointly evaluate and improve the safety of plant design and operation.

With the deterministic approach, postulated events are chosen to encompass a range of related possible initiating events which could challenge the safety of the plant, in order to define design parameters for engineered safety features. Analyses are made to investigate the effectiveness of the safety functions in the event of the accidents they are intended to control or mitigate. Conservative assumptions are made at all steps of such calculations of accidental sequences to show that the response of the plant and its safety systems to postulated events allows the plant to meet safety targets and to ensure that the end result in terms of potential releases of radioactive materials is acceptable.

Probabilistic analysis is used to evaluate the likelihood of any particular accident sequence or scenario, and its consequences. This evaluation may take into account the effects of mitigation measures, within and beyond the scope of the plant probabilistic analysis and used to identify risk and any possible weaknesses in design or operation which might dominate risk. Probabilistic methods can be used to aid in the selection of events requiring deterministic analysis.

The process is presented diagrammatically in Fig 1-1. From this figure, it can be seen that the safety case involves the integration of a traditional safety analysis and a probabilistic risk assessment. The process can be viewed as having four major elements. They are:

- Assurance that the equipment and procedures in the facility are capable of performing their assigned mission, i.e. preventing the release of hazardous materials in the presence of all credible threats to the boundaries which contain or confine them;
- Assurance that the same equipment has a high likelihood of being available and functioning at the time of the threat and that the probability of a resulting failure of confinement or containment is acceptably low;
- Consideration of all possible sequences of events and assurance that barriers are maintained or set in place to ensure the mitigation or prevention of consequences for all important accident scenarios;
- Initiation of a process to maintain the validity of all assumptions made during the capability and risk or reliability assessments, for all phases of facility operation.

Within the framework of the RA programme, during the design phase the PSA will:

- Provide a basis for cost/benefit analysis which can be used to guide the final selection of the various system or component configurations which are proposed during the evolution of the final plant design;
- Identify a critical item list which represents all systems, structures and components which are ranked in order of their importance to safety.

During plant operation, the RA programme will:

- Use a living PSA plant model to evaluate the absolute and relative merit of potential changes or alternative operational strategies and plant modifications;
- Provide quantitative guidance to the maintenance planning organisation, in combination with plant failure data:
  (i) Rank SSCs to provide a basis for a risk reduction programme;
  (ii) Rank SSCs to guide the implementation of a condition directed maintenance programme.

### 1.1.2. Technical specifications

During the performance of safety analyses and reliability assessments, the boundary conditions which are imposed on the analysis implicitly define a set of assumptions whose validity must be assured during operation of the plant. Maintaining the validity of these assumptions will require the application of administrative controls, typically imposed in the form of a set of plant technical specifications. In the current generation of Technical Specifications, these controls fall into several broad categories:

- Imposition of constraints on plant operating configuration so that the number of operable functional success paths never decreases below the minimum number assumed in the preliminary or final safety analyses (PSAR and FSAR);
- Failure to maintain this number of success paths results in the plant's entering a limiting condition for operation (LCO), a condition where the plant must either be restored to an acceptable configuration within a defined period of time, or proceed to shutdown;
- Imposition of constraints on the allowed out-of-service outage times for important SSCs. By imposing constraints on the allowed outage times (AOTs) for specific SSCs, the Technical Specifications assure an acceptable level of SSC availability.
- Imposition of functional testing, inspection and calibration requirements which provide assurance of a high level of reliability and availability for important SSCs.

This testing programme falls within the plant "surveillance testing programme" (STP) which provided the basis for testing and monitoring performance of all SSCs whose reliability and availability is important to the safety analysis.

The results from the reliability assurance programme are expected to augment the deterministic requirements of the plant technical specifications and result in the inclusion of specific restrictions on operating plant configuration, AOTs for SSCs and restrictions on SSC with regard to unavailability (cumulative outage hours per service period hours) and reliability performance criteria.

## 1.2. ECONOMICS

The primary RAP objective is to provide a plant which operates reliably and safely while generating electricity at minimum cost and fully meeting all safety requirements. The results from the RAM and PSA programmes provide the information needed to undertake cost/benefit analysis to justify and prioritize plant changes, modifications and enhancements during design and operation.

Economic evaluation, a primary constituent of the RAP decision making process, generally includes the following steps:

- Use of RAM and PSA models to determine the change in productivity or risk which is attributable to a proposed change to the plant;
- Estimating the costs of the proposed change;
- Using models to translate changes in risk and productivity to their economic equivalents;
- Comparing the expected costs and benefits which are directly attributable to a proposed change;
- Using the RAP cost/benefit assessment process to justify making the change and to prioritise its implementation, relative to other changes which have been economically justified.

The economic evaluation process can be used to justify and prioritize changes to the plant which affect both safety and capacity factor.

In undertaking an economic optimization, consideration must also be given to the evaluation of the fuel cycle and implications to the cost of construction, plant accessibility and decommissioning.

Increased demands for higher and higher levels of reliability or availability can generally only be accomplished when accompanied by an exponential increase in procurement and installation costs. This is because increasing the reliability of a very reliable system can generally only be accomplished by:

- Purchasing very reliable (expensive) components
- Adding redundancy
- Increasing diversity

However, the rewards for increasing system reliability tend to decrease exponentially as high levels of reliability are achieved as system reliability is increased.

The important implication to be drawn from the above example is that because the benefits from increased reliability tend to decrease as the costs of achieving it increase, there is an optimal point. This means that the RA programme should search for this optimum if it is to be truly successful.

## 1.3. “QUALITY” AND “RELIABILITY” ASSURANCE PROGRAMMES

The plant reliability assurance (RA) and quality assurance (QA) programmes have similar objectives, i.e. assurance of plant safety and reliability, but achieve them through different mechanisms.

The **quality assurance programme** is an interdisciplinary, documented management tool that provides a means for ensuring that all work is adequately planned, correctly performed and assessed. The QA programme documentation describes the overall measures established by an organization to achieve the management goals and objectives which are applied to every unit and individual within the organization, i.e. senior management has a responsibility and for the planning, development, and implementation and success of the QA programme by:

- Developing and issuing a written QA policy statement which clearly reflects their concepts and objectives regarding quality and commitment to the attainment and continuous improvement in quality,
- Establishing and cultivating principles that integrate quality requirements into daily work and to provide individuals performing the work with the necessary information tools, support and encouragement to perform their work properly,
- Assigning responsibility to the line organisation's goals and objectives, and empowers the individuals in the organisation to perform the task they have been assigned,
- Establishing the management's objectives for the nuclear power plant project and assigning responsibilities and authorities, defining policies and requirements and providing for the performance and assessment of work,
- Ensuring that the programme is binding on all personnel, including those with responsibility for planning, scheduling and allocating resources,
- Ensuring that the programme describes or provides reference to the organisational structure, functional responsibilities, levels of authority and interfaces for all segments of the organisation.

The **reliability assurance** programme integrates deterministic criteria and probabilistic techniques to provide predictions of the relative and absolute importance of individual plant components. Amongst other benefits, this will facilitate the implementation of "graded QA" programmes which assign resources to the achievement of "quality" which are commensurate with their importance to both economy and safety, and the implementation of Technical Specification requirements which are commensurate with their impact on plant risk.

## 1.4. DESIGN AND OPERATIONAL RELIABILITY ASSURANCE PROGRAMMES

The RA programme defines the design and operational requirements which assure acceptable levels of plant safety, and will provide a basis for many other tasks which can be used in the plant decision making processes which assure optimal plant economic performance. The guidebook will describe how to use:

- Plant-wide reliability models to predict initiating event frequencies for use in the risk assessment and to predict plant forced outage rates;
- Risk models to optimise the design of the nuclear island so that the plant is capable of meeting all defined deterministic and probabilistic safety criteria at minimum life-cycle cost;
- Results from the risk assessment to prioritise each plant component, sub-system and system in terms of its importance to risk and focus the development of procurement specifications, procurement quality requirements and construction and pre-operational testing activities on providing high reliability and maintainability for the hardware which is commensurate with its importance to safety;

- Results from the risk and reliability assessments to identify important human interactions and confirm that the training and procedural control systems focus on maximising human performance in these areas;
- Results from plant-wide reliability, availability and maintainability studies to prioritise each plant component, sub-system and system in terms of its importance to electricity generation and focus the development of procurement specifications, procurement quality requirements and construction and pre-operational testing activities on providing high reliability and maintainability for the hardware which is commensurate with its importance to economy.

## 1.5. PLANT ORGANIZATION INFRASTRUCTURE AND THE RELIABILITY ASSURANCE PROGRAMME

The relationships between the plant infrastructure and the plant can be represented graphically in the form of a "goal tree' which portrays the hierarchical relationships between:

- An unambiguously defined organisational objective;
- The sub-goals and functions which must be satisfied to meet this defined objective;
- The success paths, or physical activities which culminate in the satisfaction of at least one goal;
- The plant activities which support each success path and assure its reliability;
- Plant programmes which provide the necessary resources and impetus to assure that individual activities undertaken to manage the probability of success for each success path are effective;
- Plant policies and regulatory requirements which serve as the "forcing function" to implement programmes which ultimately will increase the probability that the overall goals and objectives will be satisfied.

The goal tree has an associated set of rules which ensure that the hierarchy between elements is maintained, because it is only by use of a strict hierarchy that the tree is able to maintains its cause-consequence nature, the very attribute which makes it useful as an analytical tool.

Figs 1-2 and 1-3 provide the structure for a simplified goal tree developed for a nuclear power generating plant. In this tree, the overall goal has been defined in terms of plant profitability, although the owner is free to define it differently if there are issues of greater importance than economy.

A review of this tree brings some important insights into focus, namely, that the human has two distinct institutional roles in the operation of a nuclear power plant:

> **Role number 1**, typified by that played by the plant control room operator.
>
> In this role, the plant operator serves as an integral part of each plant success path and becomes a prime determinant in the probability that it will operate successfully. Failure of the operator to fulfill his role correctly, e.g. actuate, shutdown or modulate system operation on demand, will result in the immediate failure of one or more operable success paths.

**Role number 2**, typified by the plant maintainer or plant trainer.

> In this second role, the plant maintainer performs a series of actions which are intended to maintain the reliability of the individual hardware elements which constitute each success path, either by periodically testing, examining, repairing or refurbishing them to maintain them as close to "as new" condition as possible. Failure of the maintainer to perform the task effectively, for whatever reason, will likely not result in immediate hardware failure, but may result in a reduction in its reliability, i.e. the SSC may fail sooner than it otherwise would have done.
>
> In this second role, the trainer performs a series of activities which are analogous to those performed by the maintainer except that they are focused on assuring the reliability of the human (operator) who is an integral part of each success path.

The trainer also trains the maintainer to improve the reliability of the human where his actions become part of a success path needed to achieve an SSC performance objective.

A RA programme does not introduce new requirements, but assures that management processes and management systems to increase the rigor and consistency in the performance of individual activities are introduced.

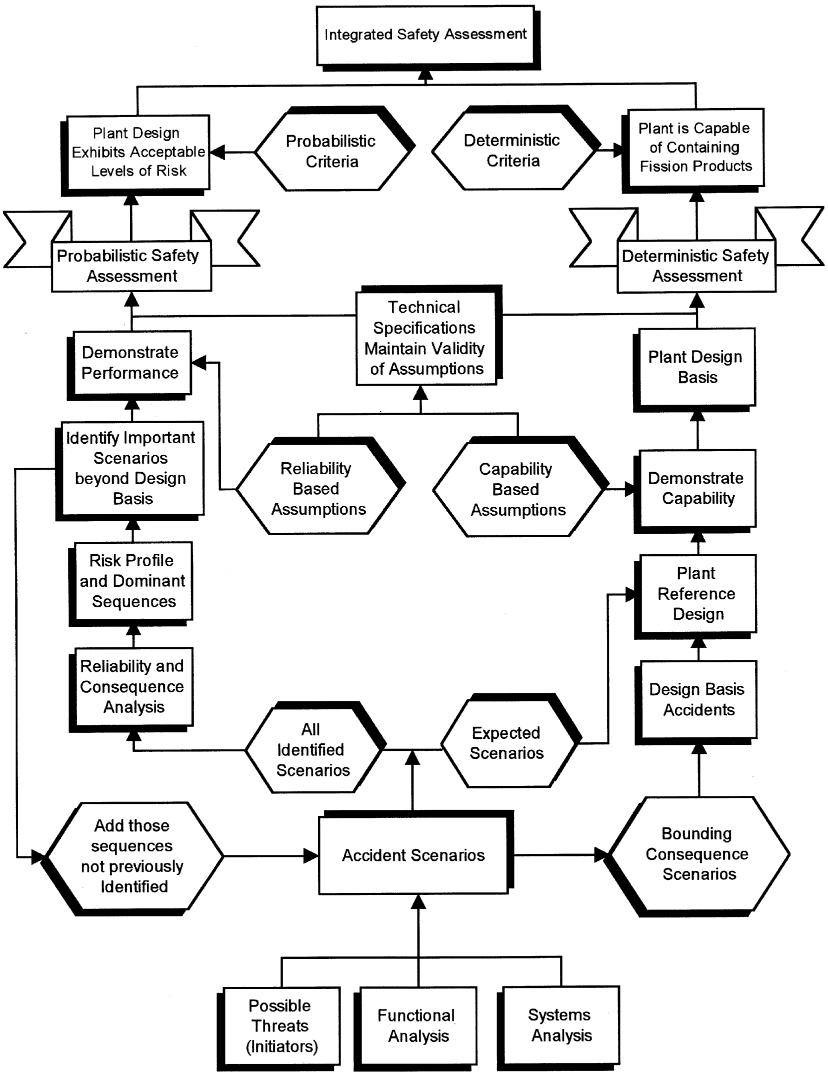

Integrated Safety Assessment
Plant Design Exhibits Acceptable Levels of Risk
Probabilistic Criteria
Deterministic Criteria
Plant is Capable of Containing Fission Products
Probabilistic Safety Assessment
Deterministic Safety Assessment
Technical Specifications Maintain Validity of Assumptions
Demonstrate Performance
Plant Design Basis
Identify Important Scenarios beyond Design Basis
Reliability Based Assumptions
Capability Based Assumptions
Demonstrate Capability
Risk Profile and Dominant Sequences
Plant Reference Design
Reliability and Consequence Analysis
Design Basis Accidents
All Identified Scenarios
Expected Scenarios
Add those sequences not previously Identified
Accident Scenarios
Bounding Consequence Scenarios
Possible Threats (Initiators)
Functional Analysis
Systems Analysis

*FIG. 1-1. Integrated safety assessment.*

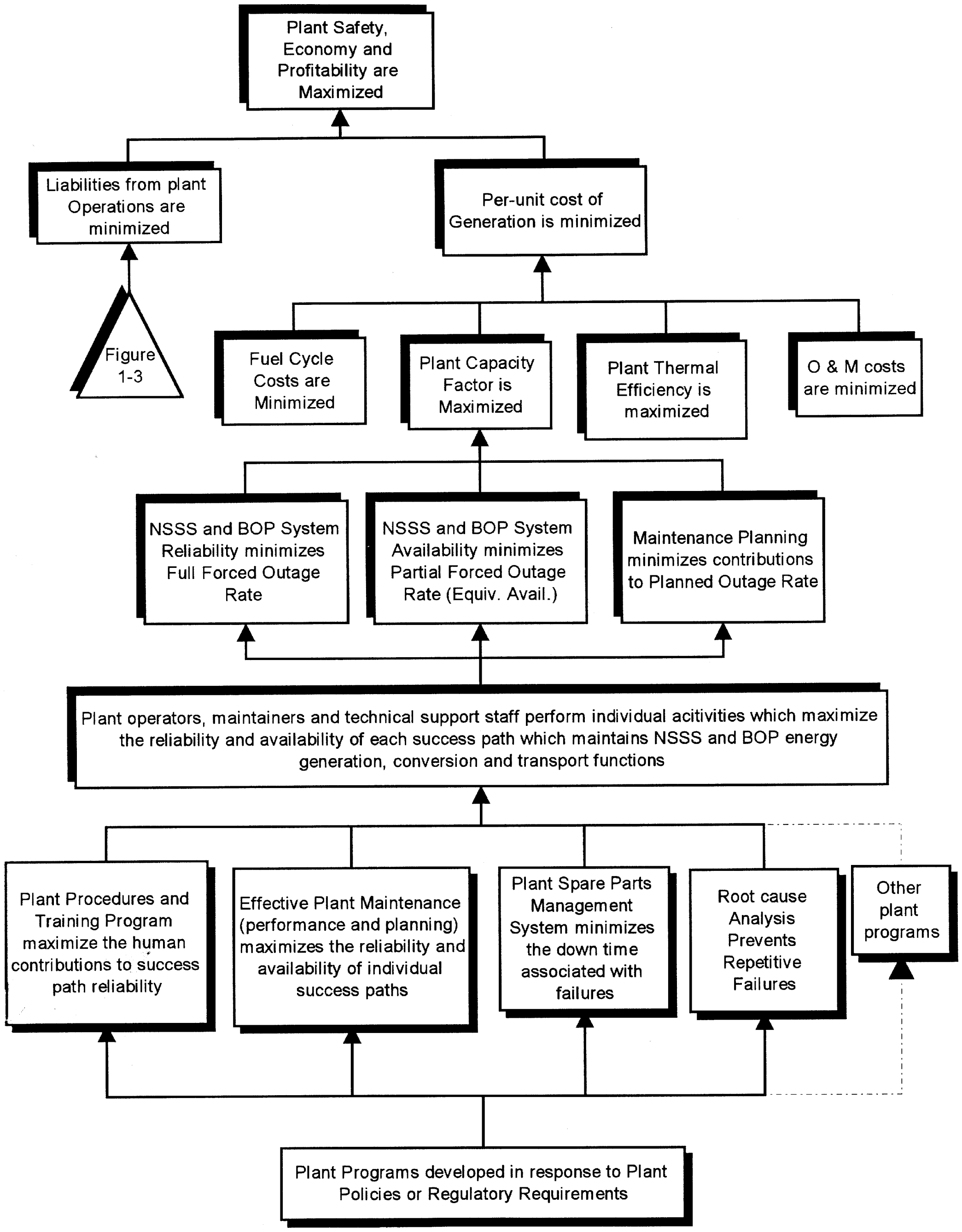

Plant Safety, Economy and Profitability are Maximized
Liabilities from plant Operations are minimized
Per-unit cost of Generation is minimized
Figure 1-3
Fuel Cycle Costs are Minimized
Plant Capacity Factor is Maximized
Plant Thermal Efficiency is maximized
O & M costs are minimized
NSSS and BOP System Reliability minimizes Full Forced Outage Rate
NSSS and BOP System Availability minimizes Partial Forced Outage Rate (Equiv. Avail.)
Maintenance Planning minimizes contributions to Planned Outage Rate
Plant operators, maintainers and technical support staff perform individual acitivities which maximize the reliability and availability of each success path which maintains NSSS and BOP energy generation, conversion and transport functions
Plant Procedures and Training Program maximize the human contributions to success path reliability
Effective Plant Maintenance (performance and planning) maximizes the reliability and availability of individual success paths
Plant Spare Parts Management System minimizes the down time associated with failures
Root cause Analysis Prevents Repetitive Failures
Other plant programs
Plant Programs developed in response to Plant Policies or Regulatory Requirements

*FIG. 1-2. Organizational goal tree — generation.*

## 1.6. STRUCTURE OF THE GUIDEBOOK

This opening section provides a broad introduction to reliability assurance. In subsequent chapters, this broad view is narrowed and each individual piece of the RA programme is described with increasing amounts of detail.

Section 2 expands the descriptions of RAP into a more detailed description of reliability assurance and initiates the discussion about the differences between RAP in design and RAP in operation. Sections 3 and 4 then go on to describe the individual design reliability assurance

(D-RAP) and operational reliability assurance (O-RAP) as they are currently envisioned. Sections 5 and 6 provide detailed descriptions of the individual sub-programmes that are likely to be key elements of a comprehensive RA programme. Section 5 describes a series of D-RAP sub-programmes and Section 6, a series of O-RA programmes.

Section 7 provides a brief description of the organizational structures which may be needed to implement RAP and provide insights which a future user can use to design his own RAP organization.

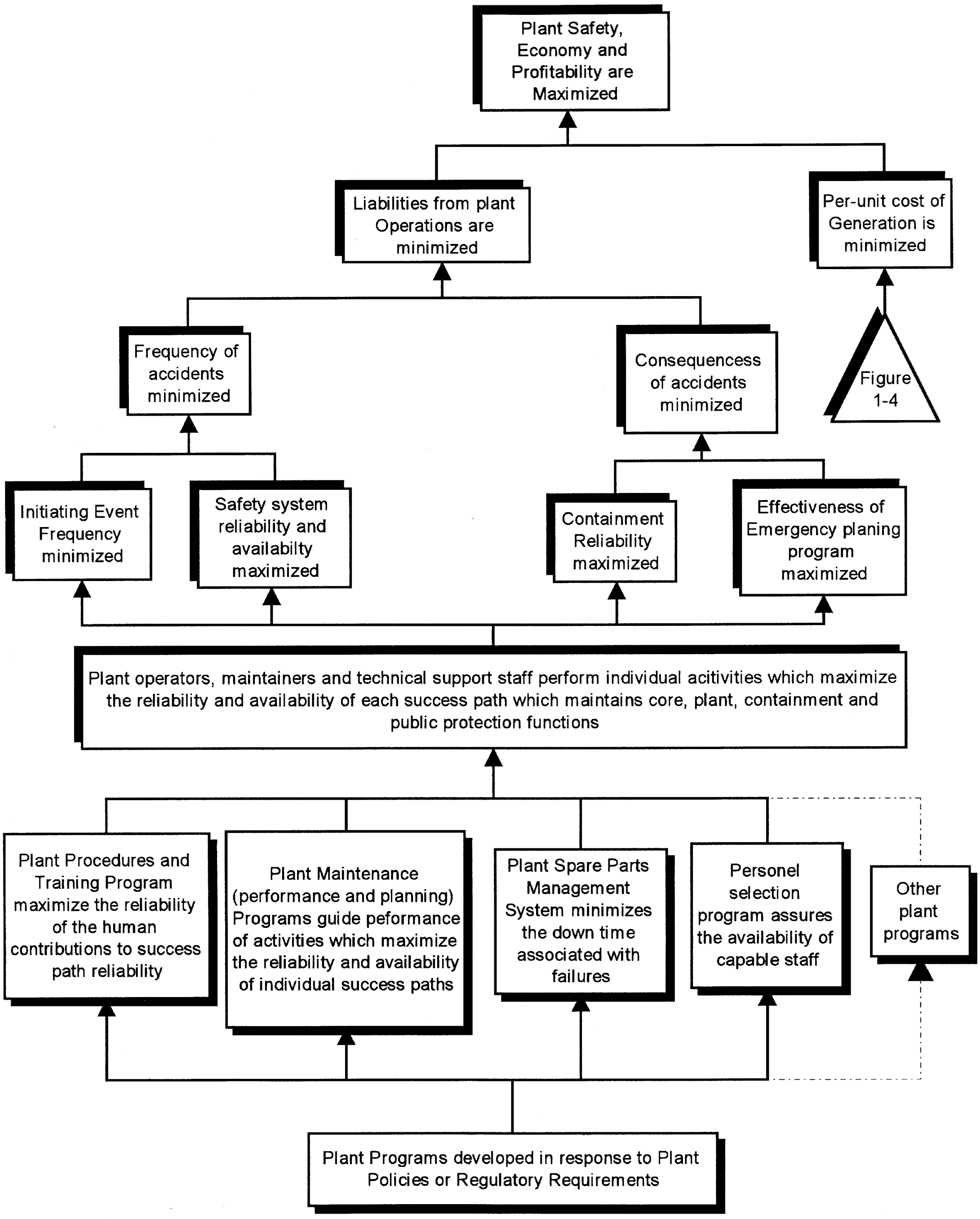

Plant Safety, Economy and Profitability are Maximized
Liabilities from plant Operations are minimized
Per-unit cost of Generation is minimized
Frequency of accidents minimized
Consequencess of accidents minimized
Figure 1-4
Initiating Event Frequency minimized
Safety system reliability and availabilty maximized
Containment Reliability maximized
Effectiveness of Emergency planing program maximized
Plant operators, maintainers and technical support staff perform individual acitivities which maximize the reliability and availability of each success path which maintains core, plant, containment and public protection functions
Plant Procedures and Training Program maximize the reliability of the human contributions to success path reliability
Plant Maintenance (performance and planning) Programs guide peformance of activities which maximize the reliability and availability of individual success paths
Plant Spare Parts Management System minimizes the down time associated with failures
Personel selection program assures the availability of capable staff
Other plant programs
Plant Programs developed in response to Plant Policies or Regulatory Requirements

*FIG. 1-3. Organizational goal tree (safety).*

# 2. OVERVIEW OF A RELIABILITY ASSURANCE PROGRAMME

## 2.1. INTRODUCTION TO RELIABILITY ASSURANCE PROGRAMME

A reliability assurance programme (RAP) is a formal management system which assures the collection of important characteristic information about plant performance throughout each phase of its life, and directs the use of this information in the implementation of analytical and management processes which are specifically designed to meet two specific objectives:

- Confirm that the plant is expected to meet, or continues to meet, each of the performance goals assigned to it by its designer, constructor, owner/operator and regulator.

  Wherever a shortcoming is detected, either because the results from an analytical task conducted during D-RAP predict that the plant design will not meet one or more of the safety, reliability or economic goals, or results from an O-RAP monitoring and evaluation programme indicate that plant performance is lower than expected, RAP activities will initiate a search for cost effective remedial measures and establish implementation criteria and commitments to achieve them.

  Where several remedial measures are possible, the D/O-RA programmes will use one or more of the analytical tools at its disposal to establish the costs and benefits from each, and provide quantitative information on the relative merits of each to the decision maker. This justification and prioritization analysis will also clearly identify those suggested improvements which are expected to incur costs which are greater than the benefits they return.

- Guide the search and implementation process for cost effective improvements to the plant to either enhance production or to reduce risk.

  In addition to serving as a performance monitoring and improvement programme, the RA programme will also focus the expenditure of resources available for performance improvement in areas where the economic return is largest, or to optimize the design and operation of the plant so that the owner receives the greatest economic return for the invested assets and operational expenses.

## 2.2. ELEMENTS OF A RELIABILITY ASSURANCE PROGRAMME

A typical reliability assurance programme can be expected to have four broad functional elements:

- Goals and performance criteria,
- Management systems and implementing procedures,
- Analytical tools and investigative methods, and,
- Information management.

### 2.2.1. Goals and performance criteria

The reliability assurance programme requires the definition and assignment of a broad set of high level plant goals and performance criteria which can be used as benchmarks for comparison with actual, or predicted, plant performance. These goals may be either deterministic or probabilistic, but, must be applicable and measurable wherever they are important to plant management systems which influence safety and economy. These goals may vary from plant to plant or from member state to member state, but will generally span the following range:

- Regulatory, societal or utility safety goals,
- Capital cost,
- Availability,
- Generation cost and,
- Radiation exposure (ALARA).

### 2.2.2. Management systems

To ensure that the RA programme produces consistent and effective results it must have:

- A set of focused goals which are consistent with the overall programme objectives, and,
- A set of management procedures and controls that establish and integrate each task which influences plant and SSC reliability and availability.

Typically these procedures will have two distinct objectives. They will:

- Ensure that the plant meets all prescribed criteria which have been imposed by corporate, industry or regulatory authorities and,
- Assure adequate quality of the products which result from each of the RAP management systems or processes.

The individual tasks, assessments and analyses which are an integral part of the D-RAP overall approach to justify and prioritize the implementation of proposed changes in hardware design, installation, service, environment and operational and maintenance practices which are intended to improve plant reliability, availability or maintainability.

### 2.2.3. Analytical tools and investigative methods

Implementation of a comprehensive RA programme requires ready access to a suite of analytical tools which can be used to predict the expected costs and benefits from potential changes to the plant. These changes can be proposed for:

- Plant layout, siting and design (e.g. redundancy, diversity, separation, control margin and support system infrastructure),
- Reliability, maintainability, availability, operability or efficiency of individual components, subsystems or systems,
- Environmental conditions (e.g. light, heat, radiation, noise, vibration) which influence component maintainability or operability,
- Containment systems,
- Waste management systems,
- Plant administrative, operating and maintenance procedures, personnel training and information systems which influence the reliability or efficiency of the man-machine interface,
- Emergency plans and severe accident management strategies,
- Outage planning procedures, methods and spare part strategies.

The range of reliability, availability, maintainability and probabilistic safety models needed to support a comprehensive RA programme is represented by the following:

- RAM models and analyses for the complete plant and for individual systems,
- Level 1, 2 and 3 PSA models, analyses and results for the complete plant,
- Economic models which use standard assumptions to relate lost generation and risk to their financial equivalents,
- Human reliability assessments and models which guide the identification of root causes for human errors and the "worth" of the relationships between enhanced plant information systems and human performance.

### 2.2.4. Information management

The effectiveness of the RAP depends very much upon the quality, accessibility and fidelity of the information used to provide the feedback to each management system about how well it is performing, and where to effect improvements. The RAP should ensure that all data collection processes are consistent with the requirements for data collection and submission to any multi-industry databases in which the plant is a participant. The plant information and database represents the knowledge from which the performance of individual plant components and systems will be derived to provide "best estimate predictions" of the worth for all proposed changes.

If a significant database is assembled for a specific plant design, then this should be the main source of data. However, in the absence of sufficient specific data, "generic" data would be used, assuming an appropriate confidence level.

This database will contain:

- Operational information about all hardware and human failure rates, restoration times, and recovery probabilities. Bayesian or statistical techniques will be used to update and maintain it current throughout the life of the plant;
- "Success criteria" which define component or system "success";
- Historical time dependent database which can be used to infer trends in both human and hardware performance, their causes and their impact (lost generation, risk, or changes in the parameters used as surrogate measures for risk).

The detailed contents of the set of plant databases which are expected to be defined and integrated by RAP process will likely need to include the following:

- Event reports for failures with potential safety significance and identification of precursors (licensee event reports (LERs) in the USA),
- SCRAM database,
- Component failure and repair databases,
- Surveillance and in-service testing records,
- Equipment history database and results from diagnostic and root cause analyses,
- Database for maintenance preventable failures,
- Safety system unavailability database,
- Human error database,
- Radiation exposure database,

- Record of plant capability and data for all curtailing failures, i.e. those which result in a loss of generation, classified by cause,
- Maintenance backlog,
- Outage records.

An overview of the interactions between each functional RA programme elements and typical plant design and operational information systems are shown diagrammatically in Figs 2-4 and 2-5.

## 2.3. APPLICATION OF THESE RELIABILITY ASSURANCE PROGRAMME ELEMENTS

The application of reliability assurance programmes in future reactors will not necessarily result in the imposition and implementation of new requirements and activities. Most elements of a RA programme are already in place and are used to manage the safe and reliable operation of the current generation reactors in all member states.

However, current approaches to reliability are often implemented in piecemeal fashion and designed to serve specific, and fairly narrow, sets of objectives.

A formal reliability assurance programme will fully integrate the plant management systems and associated activities which influence the reliability, availability or maintainability of critical SSCs whose performance is important to plant capacity factor, plant safety or plant risk.

The success of the RA programme will ultimately depend upon several factors:

- Definition of appropriate goals to describe acceptable levels of plant performance,
- Completeness, fidelity, confidence level and pedigree of the data gathered by plant information systems,
- Robustness of the analytical methods used to infer and model the cause and effect relationships which exist between plant functions, success paths, SSCs and humans,
- Inherent fidelity of the qualitative and quantitative insights provided by results obtained from each of the plant modeling processes,

Each of these RA programme sub-elements will be described in additional detail in this section to the guide because of their importance. Descriptions of the actual plant programmes which can be used to collect, analyze and present the information needed by a RA programme are provided in Sections 5 and 6.

### 2.3.1. Goal setting

During the plant design phase, the RA programme will implement procedures which guide the development of a reference set of system and plant level performance goals against which plant performance will be measured throughout its life. These goals will be consistent with, or more restrictive than, all imposed regulatory or societal goals, but, optimized to maximize the economic benefits to the plant owner/operator.

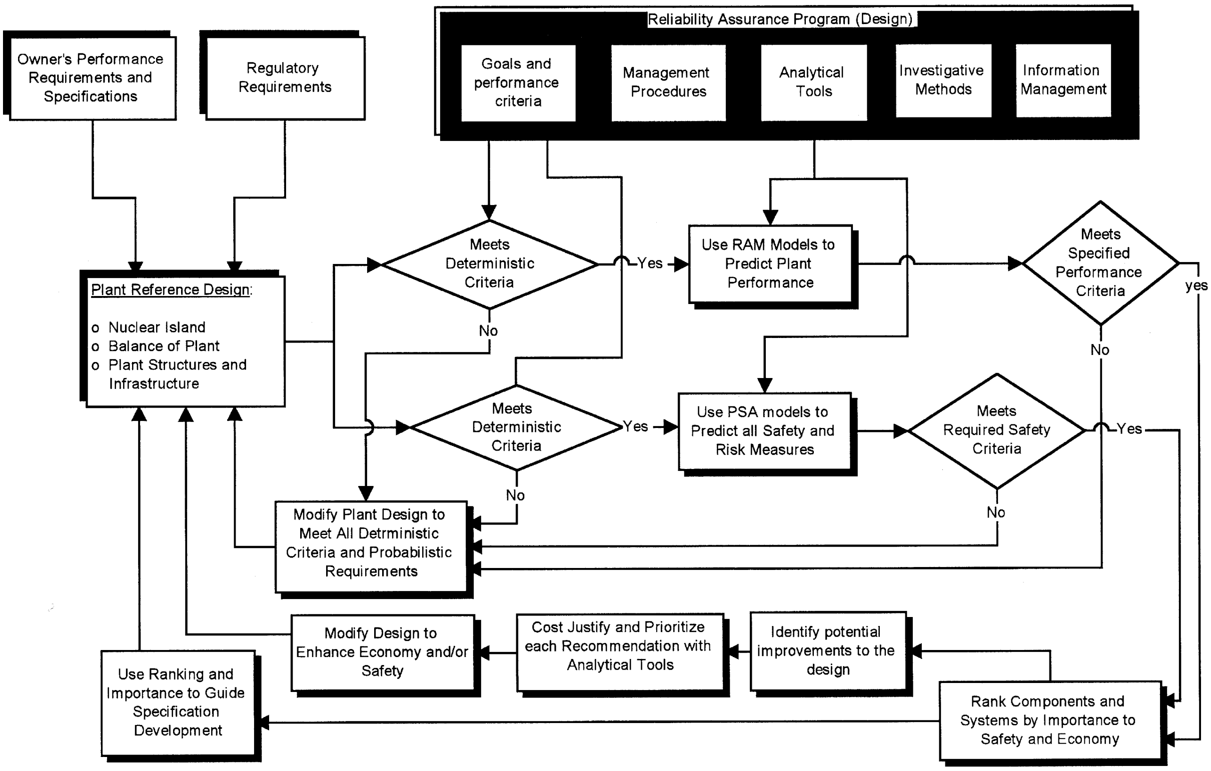

Reliability Assurance Program (Design)
Goals and performance criteria
Management Procedures
Analytical Tools
Investigative Methods
Information Management
Owner's Performance Requirements and Specifications
Regulatory Requirements
Plant Reference Design:
o Nuclear Island
o Balance of Plant
o Plant Structures and Infrastructure
Meets Deterministic Criteria
Yes
No
Use RAM Models to Predict Plant Performance
Meets Specified Performance Criteria
yes
No
Meets Deterministic Criteria
Yes
No
Use PSA models to Predict all Safety and Risk Measures
Meets Required Safety Criteria
Yes
No
Modify Plant Design to Meet All Detrministic Criteria and Probabilistic Requirements
Modify Design to Enhance Economy and/or Safety
Cost Justify and Prioritize each Recommendation with Analytical Tools
Identify potential improvements to the design
Use Ranking and Importance to Guide Specification Development
Rank Components and Systems by Importance to Safety and Economy

*FIG. 2-1. Reliability assurance applied to design (D-RAP).*

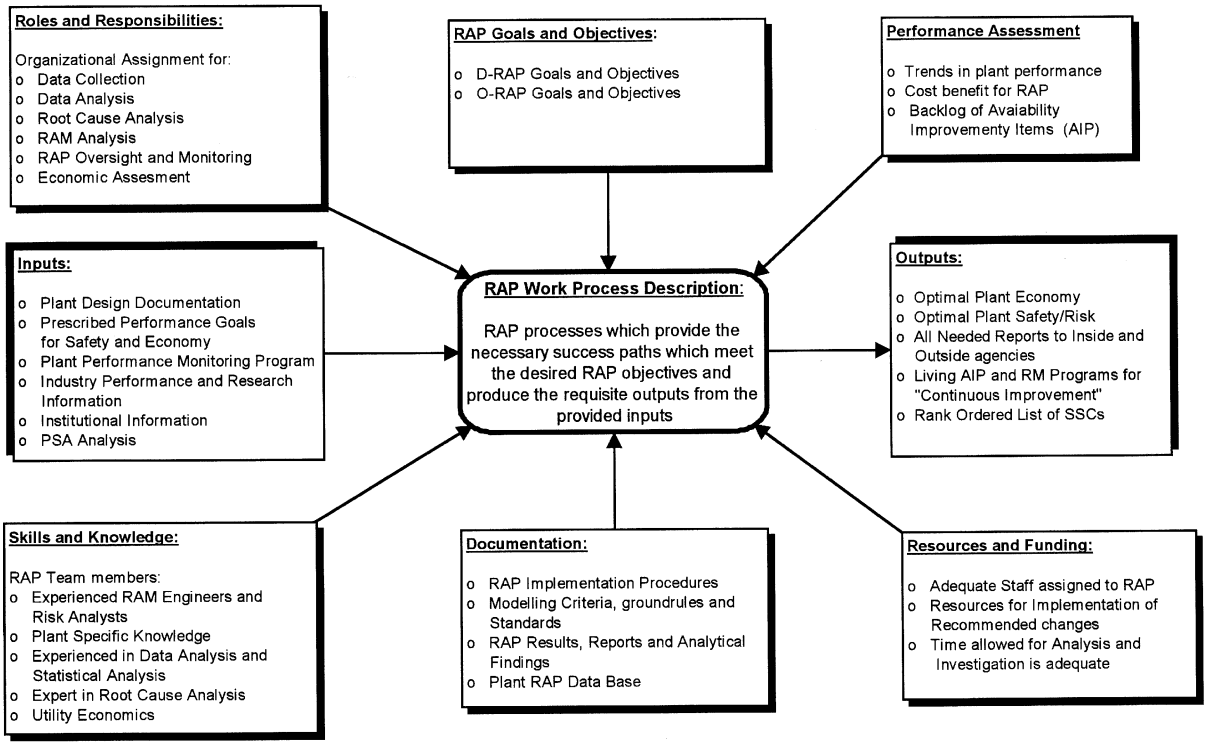

Roles and Responsibilities:
Organizational Assignment for:
o Data Collection
o Data Analysis
o Root Cause Analysis
o RAM Analysis
o RAP Oversight and Monitoring
o Economic Assesment
RAP Goals and Objectives:
o D-RAP Goals and Objectives
o O-RAP Goals and Objectives
Performance Assessment
o Trends in plant performance
o Cost benefit for RAP
o Backlog of Avaiability Improvementy Items (AIP)
Inputs:
o Plant Design Documentation
o Prescribed Performance Goals for Safety and Economy
o Plant Performance Monitoring Program
o Industry Performance and Research Information
o Institutional Information
o PSA Analysis
RAP Work Process Description:
RAP processes which provide the necessary success paths which meet the desired RAP objectives and produce the requisite outputs from the provided inputs
Outputs:
o Optimal Plant Economy
o Optimal Plant Safety/Risk
o All Needed Reports to Inside and Outside agencies
o Living AIP and RM Programs for "Continuous Improvement"
o Rank Ordered List of SSCs
Skills and Knowledge:
RAP Team members:
o Experienced RAM Engineers and Risk Analysts
o Plant Specific Knowledge
o Experienced in Data Analysis and Statistical Analysis
o Expert in Root Cause Analysis
o Utility Economics
Documentation:
o RAP Implementation Procedures
o Modelling Criteria, groundrules and Standards
o RAP Results, Reports and Analytical Findings
o Plant RAP Data Base
Resources and Funding:
o Adequate Staff assigned to RAP
o Resources for Implementation of Recommended changes
o Time allowed for Analysis and Investigation is adequate

*FIG. 2-2. Reliability assurance applied to operations (O-RAP).*

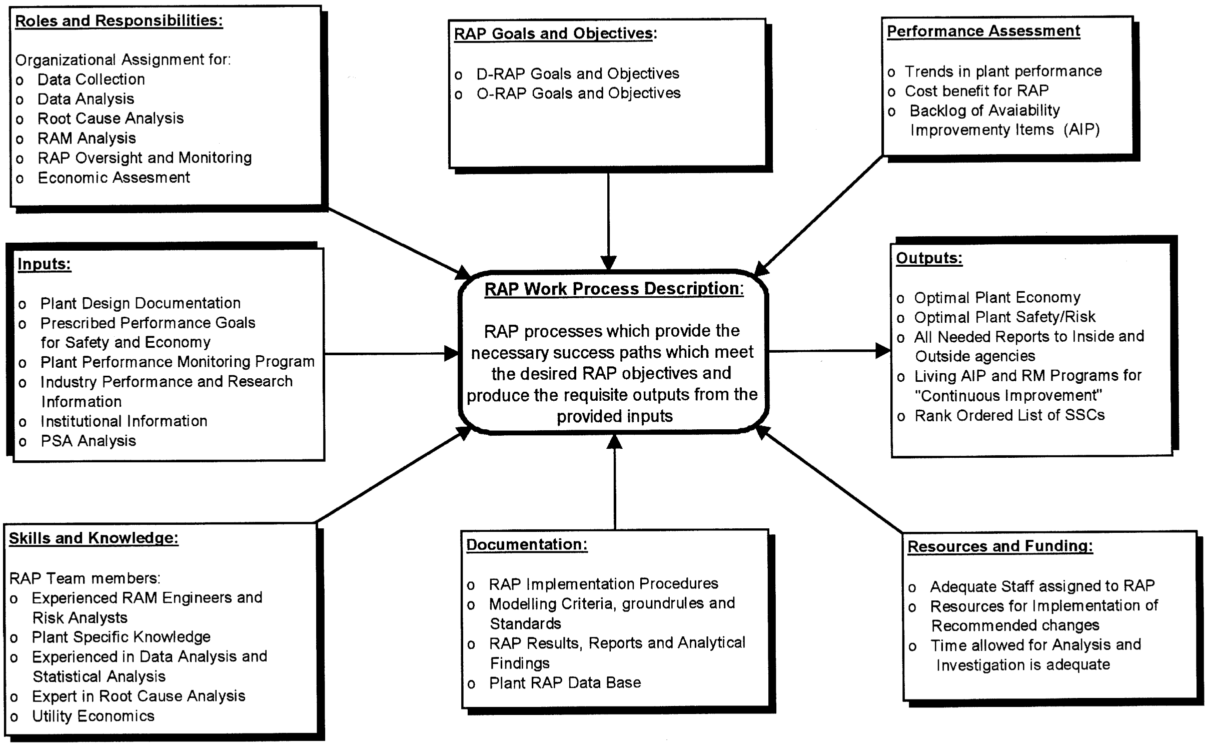

Roles and Responsibilities:
Organizational Assignment for:
o Data Collection
o Data Analysis
o Root Cause Analysis
o RAM Analysis
o RAP Oversight and Monitoring
o Economic Assesment
RAP Goals and Objectives:
o D-RAP Goals and Objectives
o O-RAP Goals and Objectives
Performance Assessment
o Trends in plant performance
o Cost benefit for RAP
o Backlog of Avaiability Improvementy Items (AIP)
Inputs:
o Plant Design Documentation
o Prescribed Performance Goals for Safety and Economy
o Plant Performance Monitoring Program
o Industry Performance and Research Information
o Institutional Information
o PSA Analysis
RAP Work Process Description:
RAP processes which provide the necessary success paths which meet the desired RAP objectives and produce the requisite outputs from the provided inputs
Outputs:
o Optimal Plant Economy
o Optimal Plant Safety/Risk
o All Needed Reports to Inside and Outside agencies
o Living AIP and RM Programs for "Continuous Improvement"
o Rank Ordered List of SSCs
Skills and Knowledge:
RAP Team members:
o Experienced RAM Engineers and Risk Analysts
o Plant Specific Knowledge
o Experienced in Data Analysis and Statistical Analysis
o Expert in Root Cause Analysis
o Utility Economics
Documentation:
o RAP Implementation Procedures
o Modelling Criteria, groundrules and Standards
o RAP Results, Reports and Analytical Findings
o Plant RAP Data Base
Resources and Funding:
o Adequate Staff assigned to RAP
o Resources for Implementation of Recommended changes
o Time allowed for Analysis and Investigation is adequate

*FIG. 2-3. Management system for RAP.*

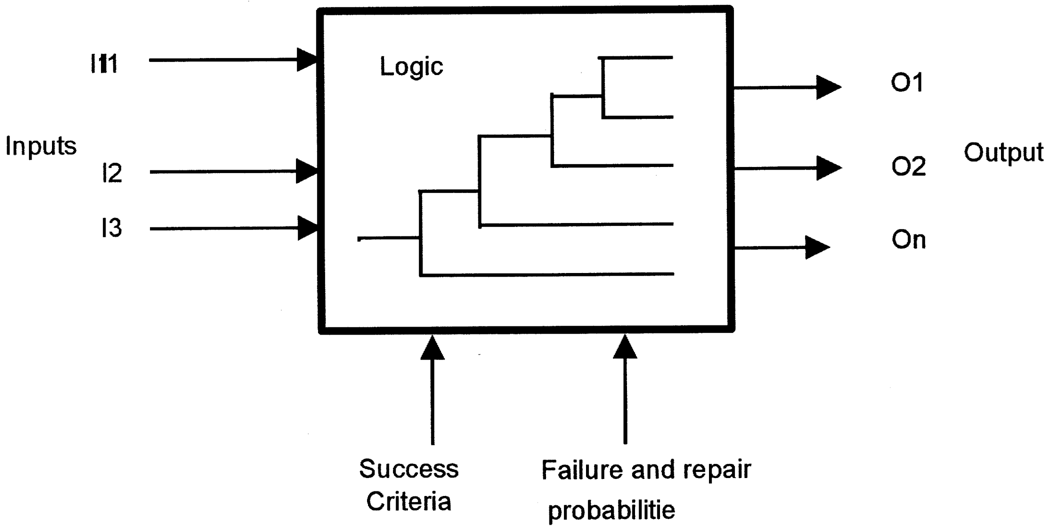


*FIG. 2-4. Example of a functional model*

The general technique for the goal setting process will require a multi-faceted approach because of the many different influences on their economic worth and sensitivity. The RAP guidebook describes a general approach which can be used to define both safety and economic goals and detail the processes by which these high level goals can be used to establish an appropriate hierarchy of performance goals which can be applied to plant systems, sub-systems, structures and components.

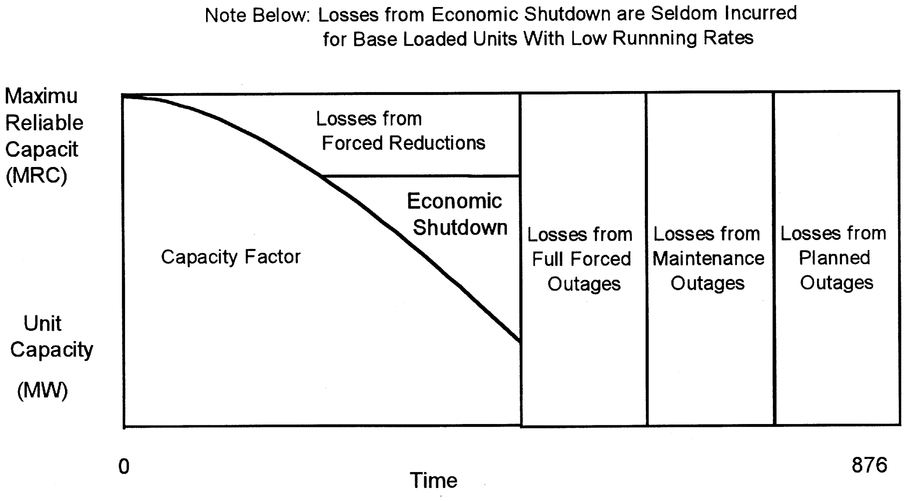


*FIG. 2-5. Unit load duration curve*

Any detailed approach towards goal setting which is ultimately selected by an individual member state must accommodate its own unique regulatory, cultural and organizational influences and national priorities.

*2.3.1.1. Safety goals*

The governing safety goals are generally defined by the national regulatory authority in the form of a set of requirements which focus on the critical safety issues:

- Limiting accidents by defining an acceptably low occurrence rate-measured as core damage frequency (CDF),
- Limiting the release of dangerous levels of radio-isotopes by defining an acceptably low occurrence rate for a large release-measured as the frequency for a large early release (LERF),
- Limiting harm to the general public by specifying acceptably low levels of individual risk, from both chronic and acute effects of radiation.

In IAEA Safety Series No. 75-INSAG-3, the safety target for existing nuclear plant in terms of a core damage frequency is below 1E-04 events per plant operating year and, for future plants, 1E-05 per plant operating year. Severe accident management and mitigation should reduce by factor of at least 10 the probability of large off-site releases.

Preliminary system goals can be derived from plant level safety goals by:

- Comparing function, system and component level information for current and advanced designs to predict any absolute or relative differences in the reliability and availability characteristics of ALWR systems, trains or components, and,
- Using the ALWR PSA and the expected ALWR train and component reliability and availability estimates to define system goals which are consistent with the overall plant safety goal.

Final system design and operational goals should be defined from quantitative insights provided by the PSA in combination with qualitative insights provided by the ALWR project team to select goals which are both challenging and feasible, i.e. achievable at a cost level which is appropriate.

#### *2.3.1.2. Productivity goals*

The utility/plant owner should select productivity goals which are achievable and demonstrated to be cost effective, i.e. provide an acceptable rate of return for the investment made in designing and operating the plant to meet these goals.

Estimates for the cost-effectiveness of the selected productivity goals can be derived from a comparison between the incremental costs and benefits expected from changes which influence plant availability, e.g. forced outage rate, planned outage rate and plant capacity factor.

The utility requirements documents suggest that a lifetime average availability of 87% meets the criteria in terms of achievability and acceptable economic returns. Within this goal are included targets for planned outage times of less than 25 days per year and forced outages of less than 5 days per year. The utility requirements set SCRAM or plant trip targets of less than one per year.

*Predicting plant reliability and availability*

Predicting the future performance of advanced nuclear plant designs to select feasible goals follows practices which are analogous to those used for “safety system goal setting”, i.e. preliminary system goals can be derived from plant level safety goals by:

- Comparing function, system and component level information for current and advanced designs to predict any absolute or relative differences in the reliability and availability characteristics of ALWR systems, trains or components, and,
- Using the ALWR RAM and outage models and the expected ALWR system, train and component reliability, availability and maintainability estimates to define system goals which are consistent with the overall plant productivity goals.

Final system design and operational productivity goals should be defined from a combination of historical experience with similar balance of plant designs, quantitative insights provided by the RAM analysis and qualitative insights provided by the ALWR project team. The selected goals should be both challenging and feasible, i.e. achievable at a cost level which is appropriate.

### 2.3.2. RAP management systems and procedures

To ensure that the RA programme produces consistent and effective results it must have a set of focused sub-objectives which are consistent with the overall programme objectives and set of management procedures and controls. These establish and integrate all of the tasks which influence plant and SSC reliability and availability during all modes of operation.

The management system which governs the implementation of the programme and provides “reliability assurance” throughout the plant should have the following explicitly defined, inputs, outputs and attributes which apply generically to all management systems:

- Identified inputs to the RAP process,
- Defined outputs from the RAP process,
- Description of the work processes which constitute the RA programme, i.e. individual tasks and sub-goals which must be done to obtain the desired outputs from the process inputs,
- Goals for the RAP management system,
- Adequate resources to implement and manage the work processes which constitute RAP,
- Defined roles and responsibilities for each organizational entity which participates in management of the RAP process,
- Adequate skills and knowledge in each organizational entity which participates in management of the process,
- Documentation of the work process so that all participants operate with a complete and coherent set of information,
- Provision for collecting and examining feedback information from the process to assess its performance and determine where improvements are needed and how they should be effected.

Fig. 2-3 provides a schematic overview of the RAP management system, as it applied to a nuclear power plant.

#### *2.3.2.1. RAP management system attributes*

The following provides a brief description of each management system attribute which must be considered during definition of the intended structure for the RAP management process, if it is to succeed.

*RAP objectives*

An appropriate definition for a RAP objective could be:

> Provide assurance that the design levels of safety, reliability, availability and maintainability for all plant SSCs meet all regulatory requirements, are cost effective, are commensurate with their importance to plant safety, reliability, risk and economy (D-RAP) and are maintained throughout the life of the plant (O-RAP).

*Adequate programme resources*

For a RA programme to be effective, it is essential that the resources assigned to it be adequate, not only in terms of numbers (budget and man-power) but, also in terms of authority and support. RAP crosses so many organizational and functional boundaries that its success will ultimately be determined by how well each plant entity fulfills its responsibilities and whether there is overall authority which can facilitate integration of activities throughout the plant.

*Roles and responsibilities*

The RAP crosses functional and organizational boundaries and, therefore it is essential that the programme clearly identify the roles and responsibilities of each participating entity. A clear understanding of organizational responsibilities is necessary to:

- Integrate the many different plant activities which influence its reliability, safety and economy and;
- Integrate the project or plant-wide collection, analysis and dissemination of information which is key to the success of the overall decision making and management processes.

*Skills and knowledge*

For a highly technical decision making programme represented by the RA programme to be successful, it is essential that the participants have adequate skills and knowledge of the techniques, tools and methods so that not only are they implemented in an appropriate way, but, they are also improved as improvements in computing hardware and the hardware used to collect and analyze information also improve.

*Documentation*

Each element of the RAP process management system must be well documented so that every participating entity (individual or organization) understands its roles, responsibilities and charter and can carry them out consistently. Documentation is also important so that whenever change is proposed to effect improvement, the context within which it is offered is clearly visible to each entity involved in the decision to accept, reject or modify it.

*Process feedback*

To achieve the lifelong goals of continuous improvement requires not only knowledge of trends in plant performance, but, also in the effectiveness of the process which is in place to see that it happens, i.e. RAP. This means that the programme must have in place a means of identifying measures of its effectiveness which can be reviewed to determine whether or not improvements are needed. Typically, these will be in the form of a set of RAP-specific performance indicators which can be monitored and analyzed on a periodic basis to demonstrate programme effectiveness.

#### *2.3.2.2. RAP procedures*

First, there will be a series of overall procedures which govern the design and operation of the plant and ensure that the deterministic requirements established either by corporate policy or regulatory authority are adhered to throughout the design and operational phase of plant life. Typically these procedures will ensure that the plant design and operation complies with:

- Requirements established by regulatory agencies;
- Utility requirements documents, design guides, industry and utility codes and standards;
- Construction guides and standards;
- Plant technical specifications or other requirements and operational constraints imposed by cognizant regulatory agencies.

Secondly, there will be a specific set of procedures which guide the performance of a defined and adequate sets of activities which are focused on ensuring the plant’s ability to meet, or exceed, the defined performance goals. This set of procedures will define the processes and protocols used to implement each management system which is part of the overall RAP. For example, these procedures will ensure that each important activity or RAP sub-programme is implemented consistently and that the products which result from these activities will achieve requisite levels of quality. Activities which will be influenced by this second set of RAP procedures will include:

- Design reviews which assure that the plant meets all specified requirements and that equipment selected for specific applications will exhibit levels of reliability, availability and maintainability which is commensurate with its importance;
- Procurement standards, specifications and evaluation processes;
- Application of "graded QA" to ensure that the QA requirements are commensurate with the benefits they return;
- Environmental Qualification (EQ) programme which assure the reliability of selected equipment during severe accidents;
- Plant administrative policies, procedures and controls which govern the selection, training, certification and procedural guidance for maintainers, operators and staff engineers (human reliability);
- Performance monitoring, performance indicators and performance based decision making practices;
- PSA and RAM analysis procedures which guide their development and application and ensure that they remain "living" tools, i.e. are continuously or periodically updated to reflect changes to the plant or changes in the way that it is operated or maintained;
- Spare parts procurement, storage and inventory management.

#### 2.3.2.3. Investigative and analytical methods and approaches

The RA programme will use a set of investigative and analytical methods and approaches to maximize the safety, reliability, availability and maintainability of important SSCs. This will be done in both D-RAP and O-RAP by identifying:

- Reasons for divergence between the actual or predicted plant or system performance and all predefined performance goals and objectives;
- Potential remedial measures, during both the design, construction, start-up and operational phases of plant life.

The following list of methods and techniques are typical of those used to effect improvement in the reliability, availability and maintainability of hardware systems either by improving diagnostic and operational planning processes or by facilitating the identification of the causes for past failures or contributors to any associated prolonged or excessive losses:

- Root cause analyses and Incident Investigations which culminate in the prevention of repetitive failures caused by weaknesses in plant management systems;
- Improved maintenance planning and improved efficiency for refueling activities on "critical path" which minimize the duration of planned maintenance and refueling outages and improved plant planned outage rate;
- "Post-mortems" or critical reviews of completed outages to improve the efficiency of future outages and to minimize plant planned outage rate;
- Root cause analysis methods to identify and prevent repetitive maintenance induced hardware failures to maximize the time between failures for important SSCs;
- Reliability/risk based configuration management system to manage safety system reliability and availability;
- Reliability, performance and condition based maintenance programmes to establish an overhaul and refurbishment schedule which prevent unanticipated failures during power operation;

– Review and optimization of the test and inspection requirements for the in-service testing (IST) and in-service inspection (ISI) programmes to minimize interference with other plant activities and minimize their contributions to planned outages.

### 2.3.3. Analytical tools

RAM and PSA models, and their associated databases provide a quantitative basis for judging the acceptability of the design, and provide the tools needed to facilitate justification and prioritization activities for all future reliability and availability decision making. The advent of enhanced analytical techniques and desk top computing capabilities during the past ten years has led to the routine use of RAM and risk assessment to guide plant decisions and their importance in achieving improved levels of both safety and economy.

#### *2.3.3.1. The role of models*

The RAM and PSA models which serve as basic computational tools for an RA programme represent mathematical analogs in which individual failure events with a one-to-one relationship to actual plant components, sub-systems and systems are logically connected to match the plant infrastructure and functional capabilities. These models are capable of quantification and can provide the frequencies and conditional probabilities for selected high level events, e.g. core damage frequency, containment failure probability or individual accident sequence frequencies, or to provide the relative and absolute importance measures for individual systems, structures and components.

The ability of RAM and PSA models to predict the net benefit which can be expected from changes to the plant or any of its institutional controls and procedures is of equal importance. This is done by modifying the model to mimic an expected post-modification configuration and re-solving it to provide the associated impacts on plant reliability, availability or risk and their associated economic values. Comparison of the predicted “worth” of the proposed modification with the cost of implementation provides the cost/benefit ratio whose magnitude can be used to both justify, and prioritize its implementation.

This ability to understand and predict the “worth” of all proposed changes to the plant is the single most important programme attribute which is used to guide the design organization towards establishing the relative merits of detail changes in their base design and in facilitating its use in the overall optimization process. This same attribute provides a plant operating staff with the ability to assess the importance of observed anomalies in hardware and human behavior and to determine where, and how, changes to the plant or its management systems will provide the greatest pay back and effect continuous programmatic and systematic improvements throughout the life of the plant.

The term “model” is used throughout this guidebook to describe these mathematical analogs to the plant, so it may be appropriate to define the term within this context. A model is any analytical tool which can mathematically represent relationships between a set of independent input and dependent output for a specified process. The process can, and frequently does, involve hardware, human or institutional activities variables because they constitute the success paths which facilitate achievement of each prescribed plant goal and objective.

Reliability models use a rigid internal logic structure to link each hardware or human event to the overall system or plant objective it serves and maintain an internal hierarchy between events. The resulting structure provides both cause-consequence qualities and serves to provide a computational structure within which the probability or frequency of occurrence of a high level, abstract, event can be synthesized from the occurrence probabilities or frequencies associated with each of its constituent, less abstract, contributors. The functional characteristics of a “model” are depicted by Fig. 2-4.

Typically:

- RAM models represent the logical relationships between each plant component, system and human action to their effects on generation and can be used to quantitatively predict the magnitude of each individual contributor to losses described by the plant load duration curve;
- Levels 1, 2 and 3 risk or probabilistic safety models, provide the logical relationships between each SSC and its effect on accident scenarios which proceed to core damage, release of fission products to the environment, or exposure of the general public to damaging radiation or radio-isotopes. These models can also synthesize a quantitative prediction of core damage frequency, conditional containment failure probability, large early fission product release frequencies and individual risks from the expected failure probabilities and frequencies predicted for individual plant SSCs.

Solution of these analytical models provides a predictive quantitative measure of the relative and absolute importance of each system, structure or component which can later be used to justify and prioritize all reliability or availability enhancement activities.

Because each RAM and PSA model is developed to provide results for a specific application, several different task-specific models may be required to span the broad spectrum of need for a comprehensive RA programme. This also implies that since the focus of RAM and PSA is quite different, each analytical approach may require different modeling techniques, methods and approaches, and failure probability data which is not necessarily interchangeable.

With each new application, changes in model inputs and outputs, the interrelationships between plant hardware, their success criteria and their failure and restoration times may be required to meet the new set of decision-making conditions and criteria. The following list of RAM and PSA model types is presented to demonstrate the potential breadth of the modeling programme which may be needed for a comprehensive RA programme.

RAP will need the results from probabilistic plant RAM models to predict:

- Losses from full and partial forced outages;
- The frequency for plant shutdowns, either as a SCRAM (manual or automatic trip, immediate shutdown (controlled, within 24 hours) or delayed (maintenance);
- Losses incurred from planned outages (refueling, overhaul and maintenance).

RAP will need deterministic models which relate component failures to their acute and chronic effects on plant generating capability. These are usually simulation models which are used to provide:

- Success criteria for equivalent availability models,
- Estimates of the times available for an operator to respond, intervene and initiate recovery from plant system upsets or component failures which can culminate in a plant SCRAM.

RAP will need the results from probabilistic safety models which:

- Predict expected core damage frequency, the frequency of fission product release to the environment and whether the plant is in compliance with all established safety goals;
- Rank each plant human action, component, sub-system and system in terms of its importance to plant risk/safety;
- Guide the selection and procurement of important pieces of hardware and provide an implication of the levels of quality assurance that may be applicable in its manufacture, installation, operation and maintenance;
- Identify, rank and understand accident sequences and use the information to guide the development of training programmes, operating procedures and emergency preparedness;
- Estimate the conditional failure probabilities for human actions associated with plant operation (productivity and safety);
- Identify maintainability issues whose resolution can reduce restoration times for important plant component, plant sub-system and systems.

The RAP will need outputs from safety models which simulate RCS transient behavior, the mechanisms and conditions associated with fuel clad and RCS pressure boundary failure, phenomenological behavior, conditions and fission product transport within primary containment, and finally the dispersion of fission products to the environment. These simulation models are used to provide:

- Guidance in selecting appropriate system success criteria for the Level 1 and 2 PSAs;
- The relative and absolute timing of events following core uncovery to provide a basis for the conditions assumed in the determination of human non-response probabilities;
- An understanding of conditions inside containment during specific accident sequences;
- Criteria for characterizing accident sequences and grouping them to estimate fission product source terms and their frequencies;
- The effects of topography, meteorology and demography on the exposure of the public to damaging levels of radiation.

#### *2.3.3.2. Economic models and their use in decision making*

RAM models provide the cause and effect relationships between the reliability, maintainability and efficiency of individual components in the power generation and conversion cycle and the generating capability of the plant. However, before specific types of models and their application to the plant economic decision making process can be discussed, a taxonomy of generic contributors to generation loss must be developed. The load duration curve, shown in Figure 2-5, has proved itself to be a convenient tool for graphically providing the basis for such a classification.

Discrimination between each potential contributor to lost generation is necessary because they have characteristic differences that require dramatically divergent modeling approaches and philosophies. The analytical issues which accompany reliability and availability modeling of normally operating systems are quite different from those of stand-by safety systems.

In the assessment of the reliability and maintainability of normally operating plant components it is important to recognize the special conditions which may result when the plant is load following, i.e. varying its generating capability to match changes in load demand.

Transition from one load to another places greater importance on the operability or controllability of the plant in intermediate power states, and during plant design it is important to ensure that equipment reliability and operability does not preclude future load following operation. Having adequate capability in the plant waste processing systems may be very important in allowing this mode of operation in some nuclear plant types.

Economic models are needed to calculate the economic costs from loss of generation, i.e. forced or planned outages and reductions. This means that a system production costing model must be used to calculate the real energy replacement and capacity replacement costs, if they are to reflect seasonal variations in load demand and the available generation mix. However, when making design decisions, such levels of precision and uncertainty are often not required. The exceptions occur whenever implementation of the decision requires a very high capital expenditure with the promise of positive, yet marginal, cost/benefit ratio.

To ensure consistency between each economic analysis it is important to use:

- Standard assumptions about future inflation rates, escalation rates and the cost of money;
- Reasonable assumptions about the plant running rate (mils/KW/h) and the average system running rates in the base year of operation;
- Average costs for installed capacity ($/KW) on the system in the base year of operation;
- Standard parameters to represent costs and benefits, e.g. equivalent capital present worth (ECPW), average annual levelized costs or revenue requirements.

For the purposes of illustration in this guide, ECPW is considered to be most appropriate because it is easy to compare one time purchase and construction costs for SSCs with the expected life-cycle return they provide in the form of increased generation or reduced operations and maintenance costs. However, the user must define the economic assumptions which are used in each analysis to assure consistency in the decision making processes.

Development of economic models for production or generation processes is straightforward because all of the information needed to perform the analysis is generally available and well understood.

Questions involving decisions about safety are generally much less clear and less well defined since the benefits are measured in terms of averted risk, a measure whose quantification requires the use of a PSA or its surrogate.

Though there are detailed descriptions of the economic models used to augment the decision making abilities of the RAM and PSA models, if D-RAP is to use them extensively in the optimization phase of design, it is important that the models have a pedigree, i.e. based on a standard set of documented economic assumptions which are to be used when calculating life cycle costs. It is more important that all economic analyses used to estimate either life cycle costs or benefits are done on a consistent basis.

Concern for consistency is as important as concern for accuracy in the prediction of costs and benefits, because provided there are no major changes in the overall time horizon within which the life cycle costs and benefits are to be estimated, the relative magnitudes of the cost/benefit relationships between decision variables are unlikely to change. Where this may represent a potential problem, sensitivity analyses can be used to better define the issue.

The economic RAM and PSA models are intended to provide information which augments, not supplants, the other inputs to the decision making process. The ultimate responsibility for making decisions must remain with the project manager and the project staff.

The detailed economic approaches and optimization methods are discussed in Section 5.

#### *2.3.3.3. RAM model use in reliability assurance programmes*

The preceding discussions imply that several different models may be needed to fully quantify each individual contributor to plant unavailability. An overview of a process which can be used to incorporate the use of RAM models into the RA programme is shown in Fig. 2-6 and an analytical process which can be used to quantify the load duration curve is shown in Fig. 2-7. Additional details about these same sets of models, and how they may be used to support the generating system RA programme are provided below.

*Plant planned outage model*

The planned outage (P.O.) model will approximate a detailed task analysis and schedule for all required refueling and maintenance activities. The model will initially be developed during the design phase and then enhanced throughout the remainder of plant life whenever additional information becomes available. The P.O. model will provide a basis for identifying equipment whose maintenance is expected to be on "critical path". The designer then has several options during plant design and component or system selection and procurement:

- Reduce the safety system maintenance load during planned maintenance and refueling outages by designing them to be maintained on-line, "at-power", without having any important effects on plant risk,
- Select components which have higher maintainability than competing products, i.e. are more easily disassembled, have less demanding maintenance activities or require maintenance less often than competing products,
- Enhance the testability and maintainability of the equipment so that the time required to perform the requisite maintenance or tests is reduced, i.e. during facility design and construction, minimize interferences, maximize lay-down areas, include provisions for rigging and access by special equipment and provide good working conditions for the maintainers (adequate heat, light and ventilation and radiation-free),
- Use reliability centered maintenance to identify the individual maintenance tasks which are necessary to ensure adequate hardware reliability and install condition monitoring instrumentation, wherever practical and justified,
- Minimize all test and maintenance activities which are prescribed by the plant licensing documents by analytically identifying those which are not necessary to maintain adequate levels of reliability, and,Use cost effective core design changes to maximize the time between plant refueling activities.

As changes to the equipment, its maintainability or testability or regulatory requirements are postulated, the effects of the changes are superimposed on the schedule and the schedule re-optimized. The benefits from schedule changes which reduce unavailability from planned outages are quantified and compared with the costs of their implementation and the cost/benefit ratio used to guide the decision makers.

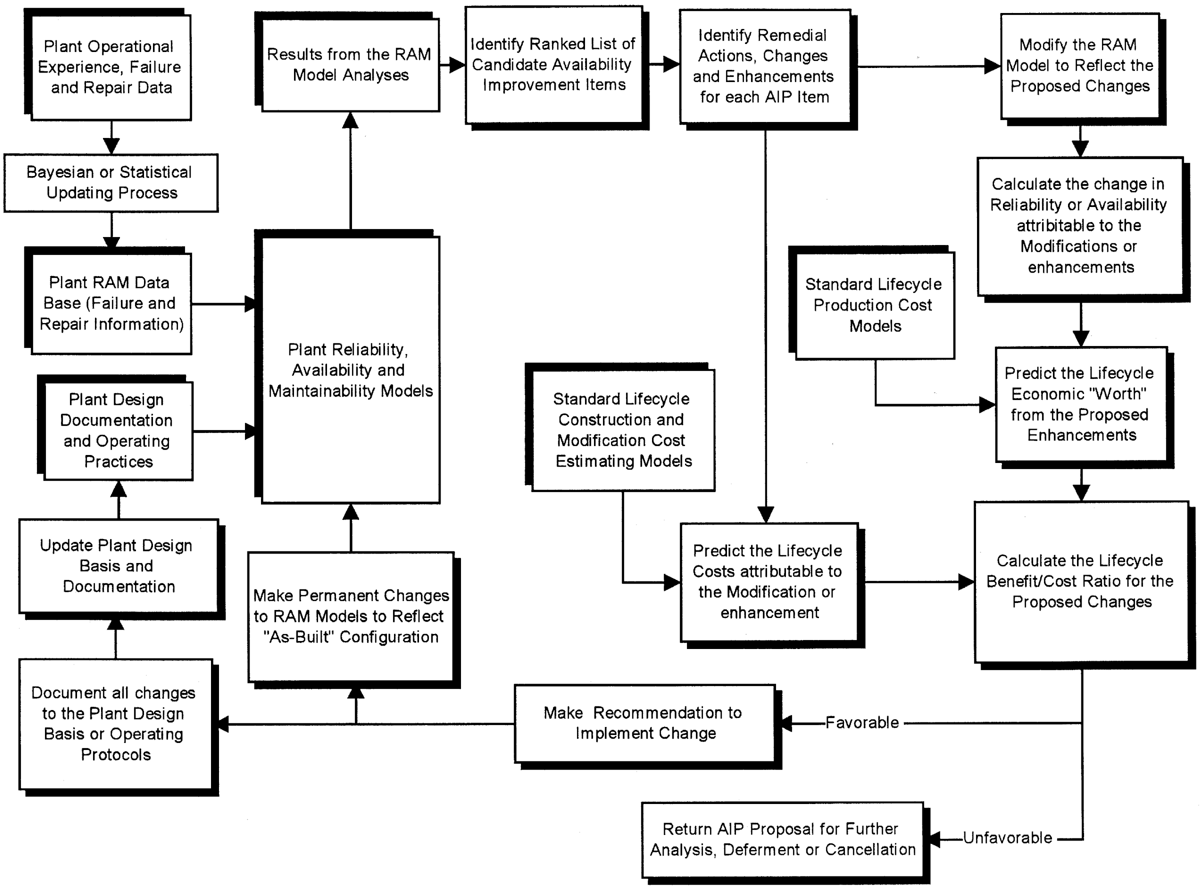

Plant Operational Experience, Failure and Repair Data
Bayesian or Statistical Updating Process
Plant RAM Data Base (Failure and Repair Information)
Plant Design Documentation and Operating Practices
Update Plant Design Basis and Documentation
Document all changes to the Plant Design Basis or Operating Protocols
Results from the RAM Model Analyses
Plant Reliability, Availability and Maintainability Models
Make Permanent Changes to RAM Models to Reflect "As-Built" Configuration
Identify Ranked List of Candidate Availability Improvement Items
Identify Remedial Actions, Changes and Enhancements for each AIP Item
Modify the RAM Model to Reflect the Proposed Changes
Calculate the change in Reliability or Availability attribitable to the Modifications or enhancements
Standard Lifecycle Production Cost Models
Predict the Lifecycle Economic "Worth" from the Proposed Enhancements
Standard Lifecycle Construction and Modification Cost Estimating Models
Predict the Lifecycle Costs attributable to the Modification or enhancement
Calculate the Lifecycle Benefit/Cost Ratio for the Proposed Changes
Make Recommendation to Implement Change
Favorable
Return AIP Proposal for Further Analysis, Deferment or Cancellation
Unfavorable

*FIG. 2-6. RAM models in reliability assurance programmes.*

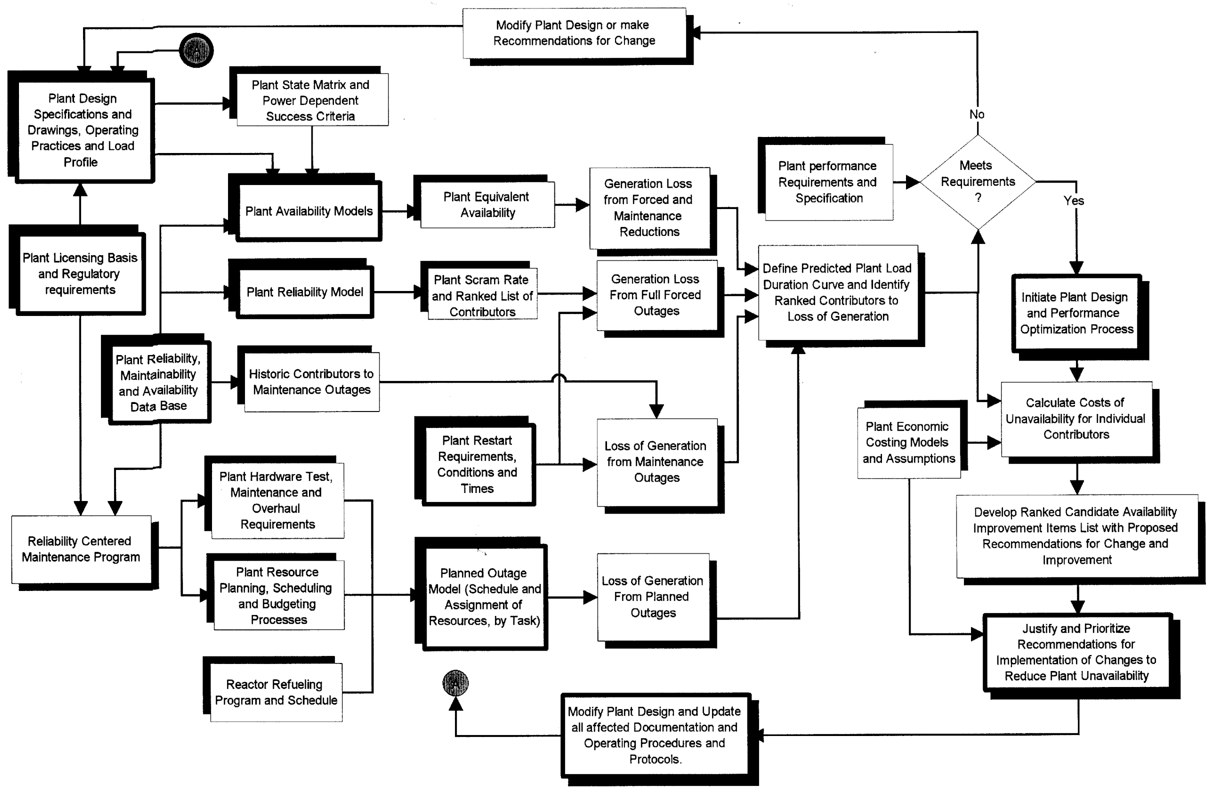

Modify Plant Design or make Recommendations for Change
Plant Design Specifications and Drawings, Operating Practices and Load Profile
Plant State Matrix and Power Dependent Success Criteria
Plant Availability Models
Plant Equivalent Availability
Generation Loss from Forced and Maintenance Reductions
Plant performance Requirements and Specification
Meets Requirements ?
No
Yes
Plant Licensing Basis and Regulatory requirements
Plant Reliability Model
Plant Scram Rate and Ranked List of Contributors
Generation Loss From Full Forced Outages
Define Predicted Plant Load Duration Curve and Identify Ranked Contributors to Loss of Generation
Initiate Plant Design and Performance Optimization Process
Plant Reliability, Maintainability and Availability Data Base
Historic Contributors to Maintenance Outages
Calculate Costs of Unavailability for Individual Contributors
Plant Economic Costing Models and Assumptions
Plant Restart Requirements, Conditions and Times
Loss of Generation from Maintenance Outages
Develop Ranked Candidate Availability Improvement Items List with Proposed Recommendations for Change and Improvement
Plant Hardware Test, Maintenance and Overhaul Requirements
Reliability Centered Maintenance Program
Plant Resource Planning, Scheduling and Budgeting Processes
Planned Outage Model (Schedule and Assignment of Resources, by Task)
Loss of Generation From Planned Outages
Justify and Prioritize Recommendations for Implementation of Changes to Reduce Plant Unavailability
Reactor Refueling Program and Schedule
Modify Plant Design and Update all affected Documentation and Operating Procedures and Protocols.

*FIG. 2-7. Use of RAM analysis to quantify the load duration curve*

After the plant is commissioned, an additional programmatic element can be used to reduce the uncertainty in future predictions of planned outage contributions to generation loss. This element comprises comparison between the "as planned" outage with the "as performed" outage. All important differences are treated to a root cause analysis to determine the reasons for the deviation and an assessment as to whether or not they could have been avoided. The identification of avoidable issues is then used to enhance the performance of the next outage. Repetitive applications of root cause analysis for several successive planned outages will result in the identification of most important contributors to extended or overlong outages and provided that the cause identification is accompanied with a recommendation and implementation programme, unavailability from planned outages will be reduced.

*Maintenance outage models*

Maintenance outage models are difficult to develop, because although their statistical contributions to plant unavailability are well documented, each one is attributed to an individual component which either suffers from a design defect which causes premature failure or experiences a random failure. This means that in the design process there is little to be done beyond compensating for past experience, i.e. use analysis of past operating experience to determine which plant components which have historically been important contributors to plant maintenance unavailability and include them on the critical plant items list. This will ensure that all steps taken during design and procurement assure that the equipment reliability and maintainability is as high as possible and that these components are included in the plant's reliability centered maintenance programme during operation.

Regulatory shutdowns may be important contributors to maintenance outages since in some cases a delayed, yet prolonged, outage may result from regulatory actions. This is likely to be unpredictable, but, again, any components whose structural or functional failure can result in an outage initiated by licensing requirements should be considered for inclusion on the plant critical items list, if it is not already there for other reasons.

*Forced outage models*

To predict the plant forced outage rate it is necessary to build a plant reliability model. This can be in the form of a reliability block diagram, fault tree, success tree, "GO" model or any other logical analogs to the plant which relates each component needed to maintain normal plant functions to continued plant operation. The model must be logically coherent so that it is capable of quantification and can be used to provide an overall prediction of plant reliability and the relative importance of each event which contributes to plant forces outages. The model must also include the possibility for operator response to dynamic events in which forewarning of a failure may result in either a plant trip or reduction in power to a new operating state. This capability may be an important factor in assessing the information needed by the operator in the control room to diagnose the causes of transient behavior and take appropriate actions to prevent shutdown.

The expected contribution to unavailability from forced outages is found from the summation of the individual occurrence frequencies for each of the important contributors to unreliability, multiplied by its associated plant down time. It is important to recognize that since each component failure results in an immediate plant shutdown, the associated restoration time is not just the time taken to repair the component, but, the total time required to return the plant to full power operation.

*Models for plant forced and maintenance reductions*

Because the effects from maintenance reductions are only discernible from past experience and difficult to predict, they are generally subsumed into the equivalent availability model used to predict the expected losses in plant from all reductions in capability. The calculations use logic models with variable success criteria to find the probability that the plant can operate successfully at each possible discrete power level to define the equivalent availability curve. The equivalent availability curve shows the probability that the plant will exceed each capability level, and integration of the curve provides the expected average capability. When the integrated value of the equivalent availability curve is multiplied by the maximum possible generation, the result is the expected annual generation.

The logic models are solved repetitively with success criteria set for each discrete power level needed to define the plant equivalent availability curve. If the logic model is solve in fault space, the individual fault events are quantified with the probability that they will be unavailable during operation, i.e. they are quantified as unavailabilities. If a logic model with success orientation is used, then event availabilities are used in the quantification process. Because the overall results from the availability analysis come from the aggregate results from a set of individual models which calculate the probability that the plant will, or will not, exceed a specific capability level, conventional measures of importance can be difficult to calculate. It is only from interpretation of the results from individual studies or power level case studies that importance can be estimated.

### *2.3.3.4. Risk model use in reliability assurance programmes*

*Risk model description*

The nuclear plant risk model, usually developed as a suite of interrelated models, is used to link the performance of each hardware and human failure to its corresponding effects on the frequency of core damage, the frequency of a fission product release and its impact on the environment in the vicinity of the plant. The results from the solution of these models is provided in the form of sets of accident scenarios, ranked in order of their importance or occurrence frequency, and absolute and relative estimates of importance for individual hardware and human failure events.

These models are typically adapted to cover the spectrum of operating modes, full power, low power, hot and cold shutdown and when appropriate mid-loop operation, a PWR operating state where the primary system is drained down to allow access for nozzle dam installation and isolation of the steam generators. The models are designed to provide a prediction of the plant response to both internal accident initiating failure events, typified by LOCAs, loss of feedwater transients and reactor SCRAMs, and external initiating events resulting from fires, earthquakes, floods, severe weather and other site specific hazards.

There are three basic interlinked elements of the complete plant risk model, (1) a model of the nuclear island which can be used to identify the frequency and nature of all important contributors to plant core damage frequency, (2) a containment model which can be used to extend each core damage scenario to include subsequential and consequential failures and predict the conditional containment failure probabilities, and (3) a consequence model which use the core damage and associated containment failure scenarios to establish the duration, magnitude and concentration of fission product release, and its associated acute and latent effects on the health of the public and environment in the vicinity of the plant.

The risk models are founded upon "best estimate" assumptions, although where there is insufficient information to define best estimate assumptions for the model, the iterative nature of risk modeling facilitates the use of a conservative approach without it necessarily having an important effect on the final results. Screening values are substituted for the failure probabilities or frequencies in areas where there is little initial information and the model re-solved. Further research to refine these screening values will only be required when the failure events appear to be important, in which case it must be confirmed that the importance is not an artifact of the assumptions but reflects real characteristics which are important to risk.

The performance of a risk assessment is iterative to eliminate the need to "know everything" before it is started. Achieving this level of knowledge "a priori" would not only be very time consuming and resource intensive but also result in inefficiency. This is because the results of every probabilistic risk assessment show that plant risk tends to be dominated by a relatively small set of the more than twenty thousand individual components which comprise an operating nuclear power plant.

The relationships between each element of the plant risk assessment, the plant design basis, the operational database and the improvement process is shown in Fig. 2-8.

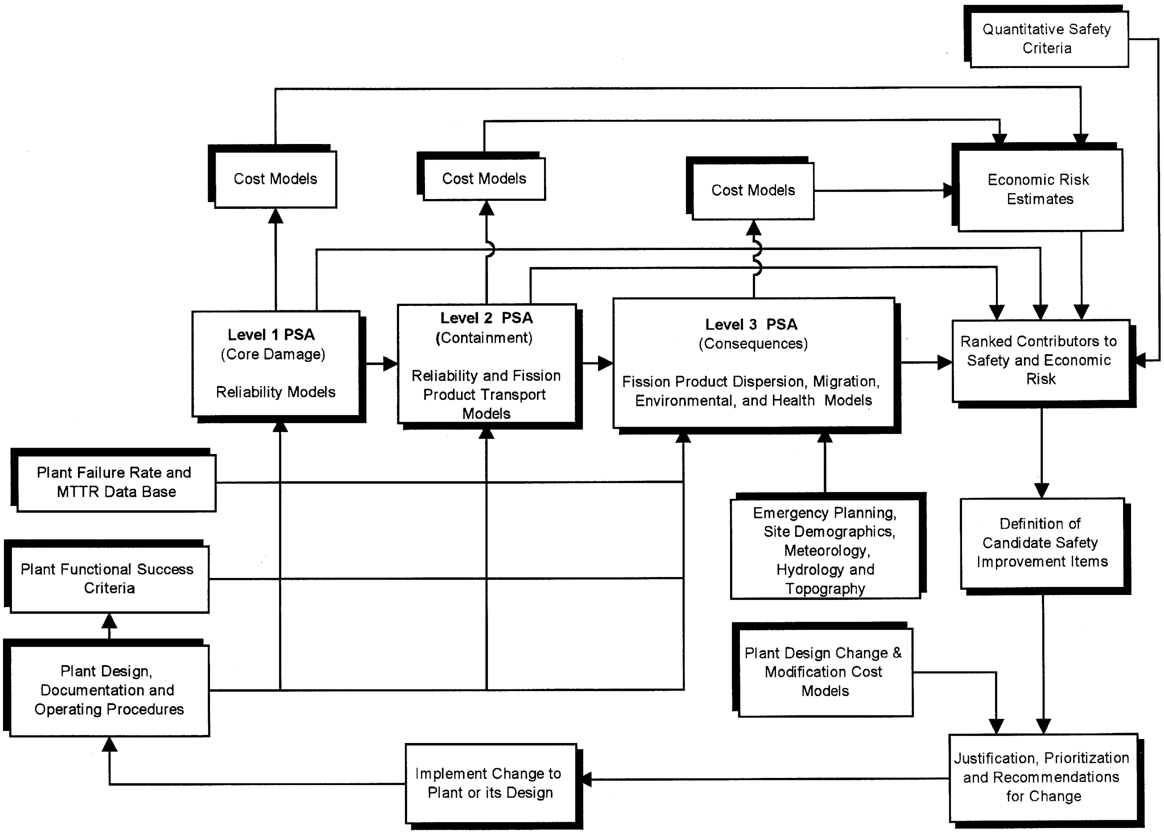

Quantitative Safety Criteria
Cost Models
Cost Models
Cost Models
Economic Risk Estimates
Level 1 PSA (Core Damage) Reliability Models
Level 2 PSA (Containment) Reliability and Fission Product Transport Models
Level 3 PSA (Consequences) Fission Product Dispersion, Migration, Environmental, and Health Models
Ranked Contributors to Safety and Economic Risk
Plant Failure Rate and MTTR Data Base
Plant Functional Success Criteria
Emergency Planning, Site Demographics, Meteorology, Hydrology and Topography
Definition of Candidate Safety Improvement Items
Plant Design, Documentation and Operating Procedures
Plant Design Change & Modification Cost Models
Implement Change to Plant or its Design
Justification, Prioritization and Recommendations for Change

*FIG. 2-8. Use of risk and reliability models in RA programmes.*

The process elements fall into four broad areas:

- Plant design basis and safety requirements,
- Plant operational information base,
- Plant risk assessment and analytical processes and,
- Plant safety improvement and risk reduction process.

*The preliminary plant reference design and the plant design basis*

The plant design basis represents the designer's product, a nuclear plant which will meet all requirements established and imposed upon the design by regulatory authorities and the commitments and needs established by the owner/operator of the facility. These requirements and commitments include:

- Probabilistic and deterministic criteria established by law to assure adequate levels of nuclear plant safety. In the United States, these requirements are established by the Code of Federal Regulations, 10CFR50, which also includes the "general design criteria", the fundamental set of requirements for nuclear plant design and construction. Other member states have their own specific requirements which are analogous to those established by 10CFR50 or augmented by other criteria which have a foundation in their assurance of acceptable levels of risk to the health and safety of the general public and the environment;
- Deterministic criteria imposed by environmental regulatory agencies, both at the federal and local levels, which ensure that all emissions from the plant conform to established standards;
- The basis and assumptions used to assure that the plant meets all regulatory requirements to a degree which is commensurate with the plants ability to function safely when the site specific characteristics and threats have been considered.
- Industry codes and standards are used in definition of the design to assure adequate design margins and appropriate selection of materials.
- Insights provided from industry research activities, which influence the selection of equipment and their assembly into functional success paths which have requisite minimum levels of reliability;
- Utility or owner/operator requirements which relate to the levels of risk which it is willing to assume, and preferences in operability and maintainability styles — perhaps to maintain consistency between the design of all of its operating plants;
- Utility preferences in control philosophy and the degree to which control remains in the hands of a control room operator or is delegated directly to the plant computer with the operator assuming the role of an "operations manager";
- The basic NSSS design offered by the selected vendor to match the defined thermal power;
- The basic energy conversion cycle (turbine/generator set) design offered by the selected vendor to meet both the load and efficiency requirements specified by the owner-operator for the steam conditions specified by the NSSS vendor.

The plant designer uses his experience and the requirements imposed above and translates it into the first preliminary design. The reliability assurance programme will superimpose its own requirements on this design. Typically these requirements will come from a "utility requirements document" (URD) which has been developed from past experience to provide assurance that specific issues will be incorporated into the design from the onset. There is little attempt at this point to determine whether the requirements are cost effective. Later in the optimization of the design phase, these requirements will be examined to confirm cost effectiveness or to implement system or component level requirements which are only described in general term by the URDs. The URDs represent the first element of the reliability assurance programme.

#### *2.3.3.5. Assessment of the preliminary plant design*

The preliminary plant design addresses the basic plant layout, the systems to be implemented, requirements for redundancy, diversity and separation and the philosophy to be adopted for an effective man-machine interface. It is this model which becomes the basis for analysis to confirm that all probabilistic performance or safety criteria are expected to be satisfied by the proposed design. Three analyses will be conducted:

A preliminary safety analysis which confirms that the preliminary design includes:

- Systems and components which are capable of preventing failure of the fuel clad when each set of specified transient events and their associated boundary conditions is assumed;
- Active and passive containment systems and structures are capable of preventing the release of fission products following a failure of the fuel clad and a loss of integrity in the primary circuit for each set of assumed transient events and their associated boundary conditions.

A preliminary reliability, availability and maintainability analysis which confirms that the plant can be expected to meet the quantitative performance goals established for the design:

- Capacity factor,
- Forced outage rates and equivalent availability,
- Planned outage rates.

Combination of the results and insights provided by each of these analyses will be used to define a preliminary ranked list of systems, structures and components which are important to plant safety and its economic performance. This information about the relative and absolute importance of SSCs can be used to focus final system design activities in the areas of greatest importance to guide component selection and procurement processes and ensure that increased levels of reliability, availability and maintainability are sought wherever they are justified and desirable.

#### *2.3.3.6. Evolution of the PSA during the design process*

One of the commonly held misconceptions involving the use of PSA during the preliminary plant design phase is that performance of the PSA cannot be initiated until the design is finalized. Lack of adequate information is quoted as the dominant reason. One process which can be used to develop the initial plant PSA models and update them throughout the design phase is shown in Fig. 2-9. A description of this process follows.

*Analysis definition and information collection*

The PSA development process for the preliminary design begins as does any other PSA, with clear definition of the scope, content and analytical objectives for the analysis which are derived directly from the applications for which the completed PSA will be used. This assessment of the expected applications for the completed study will also provide an indicationof the number of discrete plant states which need to be examined within the PSA and the extent to which external threats should be initially considered.

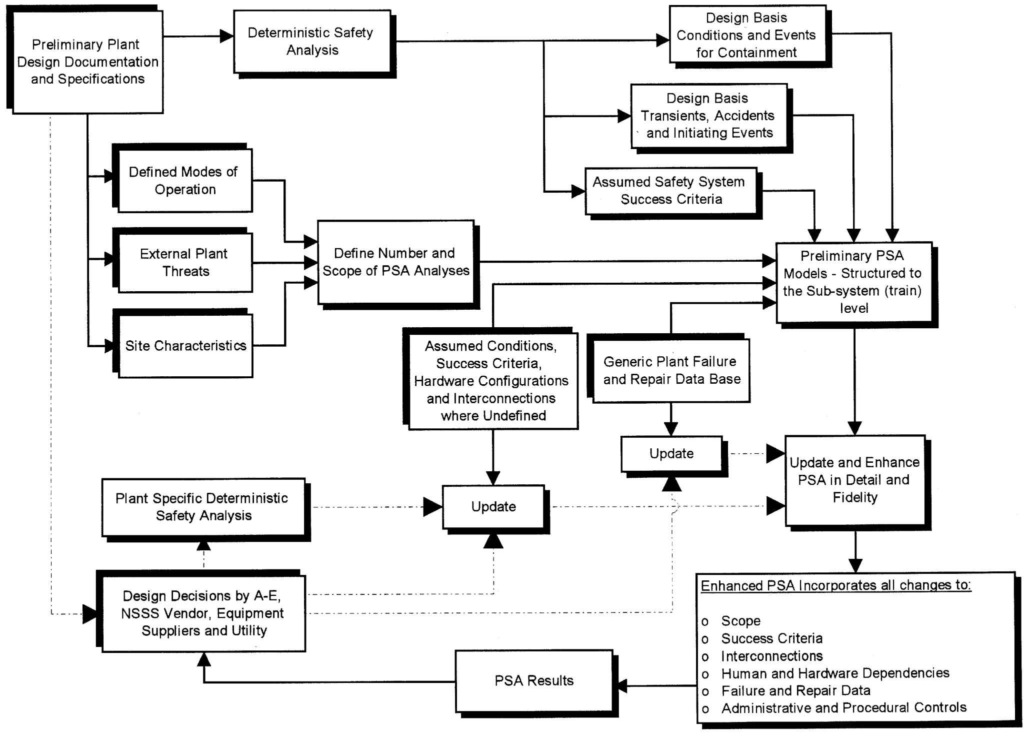

Preliminary Plant Design Documentation and Specifications
Deterministic Safety Analysis
Design Basis Conditions and Events for Containment
Design Basis Transients, Accidents and Initiating Events
Assumed Safety System Success Criteria
Defined Modes of Operation
External Plant Threats
Site Characteristics
Define Number and Scope of PSA Analyses
Preliminary PSA Models - Structured to the Sub-system (train) level
Assumed Conditions, Success Criteria, Hardware Configurations and Interconnections where Undefined
Generic Plant Failure and Repair Data Base
Update
Update and Enhance PSA in Detail and Fidelity
Plant Specific Deterministic Safety Analysis
Update
Design Decisions by A-E, NSSS Vendor, Equipment Suppliers and Utility
Enhanced PSA Incorporates all changes to:
o Scope
o Success Criteria
o Interconnections
o Human and Hardware Dependencies
o Failure and Repair Data
o Administrative and Procedural Controls
PSA Results

*FIG. 2-9. PSA* update *during design.*

Decisions about PSA scope and content will be tempered by the plant specific licensing issues and whether there are any unique site characteristics which introduce potentially large uncertainties in the reliability of systems providing core or plant protective functions, the ability to evacuate or protect the public or the degree of flexibility in defining an appropriate emergency planning zone for the plant.

Following definition of the analytical scope, content and any associated simplifications, all the information about the plant is gathered and sorted to provide the basis for the models. Since individual components and design details are generally undefined, the models will be constructed to represent the basic reliability structure of the plant, namely:

- Accident initiating events or events which threaten normal core and plant protective functions;
- The primary success paths which maintain the critical functions after a plant upset, (transient, LOCA and SCRAM);
- (The plant support system infrastructure which provides information, power, control, actuation, and cooling to the primary success paths.

Discrimination or detail in the model will typically be to the sub-system or train level, and represent groups of (undefined) components which logically exist as series elements within each sub-system. Generally, the design basis will provide the basic plant information from which the PSA models will be derived, and the success criteria will be derived from the results of the safety analysis performed to confirm design capability. In the event that the details are still not adequate, the PSA modeler makes assumptions about how the plant will likely be designed. These assumptions will be based on the actual design philosophy employed in other plants which have the same NSSS vendor or were designed by the same architect engineers, or reflect a degree of redundancy, diversity and separation which appears needed to meet the overall safety criteria.

Quantification of the models will require a failure, repair and test database. Initially, this data will be determined from generic sources or from other appropriate plant databases. Only in a revolutionary design, rather than evolutionary design, will there be a need for failure and repair data for components which have little or no operating experience. In these cases, results from prototypical testing may be all that is available to guide the estimation of likely reliability and maintainability parameters from expert opinion.

The bottom line, throughout the model construction phase, is that the PSA analyst makes assumptions about the plant reliability structure which best express the existing state of knowledge. These models are updated as the plant design matures, and increased details become known. Since the basic model reflects only the reliability structure of the plant, updating becomes a relatively simple task which can be done quickly, so that insights gained during the periodic re-solution of the models can quickly be fed back to the design team to keep them apprised of the effects of their design decisions.

These same insights gained during the periodic update and resolution of the models can also be used to focus the design team's attention on potential vulnerabilities or areas of importance to risk. This facilitates the team's ability to find and fix problems AS EARLY AS POSSIBLE during the design process. **The costs of correcting design flaws tends to increase exponentially during each phase of plant life**, i.e. a rule of thumb indicates that for each dollar used to correct a flaw detected during the preliminary design, it will cost approximately one thousand dollars to correct this same problem if it remains undiscovered until the plant enters the commissioning or operational phase of its life.

### *2.3.3.7. Use of the "Living" PSA (L-PSA) during operations*

The reliability assurance programme will rely heavily on the use of the plant PSA to guide the operational decision making process. As a result, it is important that this PSA is routinely updated to reflect all changes to the plant, failure and repair data and any other operational information which is likely to influence the failure probabilities of risk important SSCs. The OECD report on the state of "living" PSA (OECD-PWGS, task 96-1) provides several findings and insights about this important issue:

- Successful L-PSA is closely related to practical plant specific use by the utility;
- Beneficial real plant specific uses possible at different levels of L-PSA, such as long term safety planning, off-line risk planning of operational activities, on-line and off-line risk monitoring and analysis of plant performance;
- A common understanding on the L-PSA approach among utilities, authorities and external PSA organizations is helpful in development of practical use of PSA;
- Effective L-PSA application programmes will require an accompanying model and tool development programme and which can tailor the PSA to meet all changes in plant operational needs.

Because O-RAP is expected to make extensive use of a living PSA, it will likely have to be extended to include the following attributes, identified by this same OECD report, the L-PSA should:

- Combine different aspects of safety and availability decision making processes;
- Combine qualitative insights with the quantitative results it provides in decision making processes;

- Provide a clear interpretation of the magnitudes and meanings of uncertainties, present in the quantitative estimates it provides;
- Provide procedural guidance as to how the L-PSA is to be used;
- Define the levels of quality assurance which must be maintained in the L-PSA.

### 2.3.4. Plant information and database

The quality of the qualitative and quantitative results provided by each of the analytical models depends entirely upon the quality of the information used in its development and quantification. In this case, the quality of information is measured directly by how well it reflects or characterizes the performance of actual plant SSCs and human institutional activities. The information needed to meet these modeling needs is generally stored in a series of databases which not only provide clear distinction between the information associated with individual SSCs but also facilitates its access by individual users.

Each modeling technique has its own special need for a comprehensive database to provide the information needed to infer failure rates and failure probabilities for the SSCs which are used in the quantification of each associated model.

There is an important difference between the information needs for the deterministic and probabilistic assessments. Plant specific information which is used to develop the deterministic models, primarily reflects:

- Phenomenological, functional or correlated thermo-dynamic-hydraulic behavior derived from first principles or from experiment;
- Information about geometric relationships, functional capability and the physical arrangement of hardware and;
- Ambient, environmental or boundary conditions which are assumed for the analysis.

This needed information is largely derived from plant drawings, specifications, operating and system descriptions and industry literature which describes research and results from experiments which have been undertaken to better understand severe accident behavior or to benchmark computer simulation codes. Information used in deterministic analyses tends to be static, i.e. generally does not change during the life of the plant and is stored in a model specific database which is part of the plant simulation model documentation.

Plant specific information associated with development of the probabilistic models has both constant and variable characteristics:

- Information relating to the logical or “reliability” structure of the plant remains relatively constant over the life of the plant because it relates very much to the physical plant, however,
- Information related to descriptions of “how well this hardware performs” is extremely variable because how well a component works, i.e. how often it fails, or how long it takes for repair following a failure, depends upon many external conditions and influences.

#### *2.3.4.1. Influences on SSC reliability and availability*

The two parameters commonly used to characterize SSC reliability and availability are mean time between failures (MTBF), and mean time to repair (MTTR) following a failure. These parameters are affected by:

- Design, manufacturing and installation differences;
- Ageing and wear-out mechanisms which in turn are influenced by material interactions between the hardware, the process and its operating environment, and how well suited the SSC is to its specific application;
- The quality of maintenance and the plant maintainers' abilities to return the component to "as new" after each refurbishment or repair;
- The quality of diagnostic and root cause programmes which identify the causes of hardware failure the first time failure occurs, and the quality of corrective action programmes which are implemented to prevent its re-occurrence;
- The quality of plant programmes which can detect incipient failures and initiate remedial action before catastrophic (long repair time) failure occurs;
- The availability and expertise of maintainers which are able to respond after a failure is detected, and whether the plant can provide the requisite logistical support (procedures, parts, tools and other equipment) in a timely manner.

The plant database will contain several sets of information which may have distinctly different characteristics.

- First, the data must provide a documented basis for the calculation of plant transient event frequencies, because these events contribute to both forced outage rates and accident initiating event rates,
- Second, the data must provide the information needed to calculate the failure probabilities for each basic event, i.e. the lowest level of failure event, which appears in each of the models and,
- Third, the database should include the time required to restore the equipment to operability following its failure, so that the effects of repair can be used to determine generating and safety system availabilities.

Development of the plant database will be initiated during the design process, and populated with information which is derived from other, non-plant specific sources, and screened or modified to adapt it to the unique plant specific conditions which are expected to occur. Sometimes this task will also entail the statistical processing of large pools of data to develop distributions of failure rates and restoration times which have known levels of numerical uncertainty.

At first, this database will remain "generic" and likely not represent the experience which is ultimately realized during reactor plant operation. However, continued collection of information about factors which influence hardware and human performance throughout plant procurement, construction and start-up, will provide a basis for its transformation into the analyst's best estimate of the actual behavior which can be expected.

The actual method selected to modify the data to make it more "realistic" will depend upon the analyst's familiarity and access to the raw data from which the average values and dispersion factors have been derived. There are several broad methodological approaches which can be used to transform "generic" equipment performance into data which is representative of that expected during actual operation. Some are briefly described below.

(1) Elicitation of expert opinion to provide unreliability and maintainability data

Expected component and system failure rates and restoration times can be elicited from an "expert" or group of experts who use their practical and comprehensive understanding of how plant and process conditions influence failure rates and restoration. Use of expert opinion can be considered a holistic form of internal Bayesian analysis but, should always employ a consistent, iterative, polling process which allows the opportunity for individual experts to achieve a consensus. The "Delphi approach" may be the best known of these types of elicitation processes.

(2) Data screening

Data screening provides a way to better adapt a "generic" database to a specific plan by screening out failure events which are not applicable because of different design or operating conditions. The failure events are statistically processed to provide a modified data which can provide a partial solution to the problem of finding information for new or different designs. The extent to which this is possible will depend very much on how well the data heritage is known and whether there is enough detail to allow data screening to occur.

(3) Data pooling

If several relatively sparsely populated sources of data are available, it may be possible to adapt them to a plant specific situation and reduce their overall levels of uncertainty by pooling them. Pooling implies the confirmation of the applicability of each source and their formal statistical combination to provide a new database which better matches the expected plant characteristics.

(4) Bayesian database updating

In the Bayesian updating process, each piece of available plant specific information is combined probabilistically with industry, vendor, reactor type or utility specific failure information to provide conditional failure rates and restoration times which are applicable to a new design.

With each of the above methods, historical levels of hardware reliability and maintainability are used to form the basis for the prediction of the future performance of a plant under a set of specified conditions. Bayesian data processing can generally can be expected to provide the best estimate of plant failure rates for future reactor designs which have little or no operational experience, because they allow the explicit inclusion of all possible influences on hardware performance which are expected in a new design.

*Preoccupation with development of the "ultimate" database*

Use of comprehensive database updating techniques can be time consuming and expensive if performed on a broad scale. Generally these processes are reserved components which are important to risk and a capacity factor or for components which are new and different, i.e. have a new, untried, design, are made of new and different materials or are used in new applications. To optimize the time and resources spent on database development and updating, RAM and PSA analyses use an iterative approach:

- Initially, the RAM and PSA models are quantified with screening or generic values which assure over prediction of failure rates and restoration times, to find out which SSCs are, or, are not, important,
- SSCs found to be unimportant with unduly pessimistic failure rates and restoration times will remain unimportant no matter how much additional data processing is

employed. Further data refinement is only necessary for those failure events which have initial importance,

- For SSCs exhibiting high levels of importance, the analyst first confirms that the importance is real and not an artifact of the assumptions made about their expected reliability, maintainability and availability, and then applies one or more of the processing methods to transform the data to become a better predictor of future hardware performance under the expected plant conditions.

## 2.4. ADVANCED TOOLS FOR RELIABILITY ASSURANCE

Integrated logistic support (ILS) is one of the new tools which have been adapted from other industries to support RA. The concept of ILS was first introduced by the US Army for its weapons systems and their field support, and has since has been established as standard practice in many different industries, i.e. aircraft, ground transportation and some large utility organizations.

Integrated logistic support is a management function which provides the initial planning, funding and controls which help to assure that the ultimate consumer or user receives a system that will not only meet performance requirements but, can be supported expeditiously and economically through its programmed life-cycle. Assurance of the integration of the various elements of support is an important ILS objective, i.e. integrating:

- Manpower and personnel,
- Training and training support,
- Spare and repair parts and related inventories,
- Test and support equipment,
- Maintenance facilities,
- Transportation and handling,
- Computer resources and technical data.

ILS has been defined as a “disciplined, unified and iterative process to the necessary management of technical activities, such as:

- Integrate support considerations into system and equipment design;
- Develop support requirements that are related consistently to readiness objectives, to design, and to each other;
- Acquire the required support and;
- Provide the required support during the operational phase at minimum cost.

Included within the concept of ILS is the element of “design for supportability” and the requirements in this area include considering maintainability characteristics in the final design.

# 3. THE RELIABILITY ASSURANCE PROGRAMME FOR DESIGN (D-RAP)

## 3.1. INTRODUCTION

Section 2 provided insight into the overall reliability assurance process, the tools which can be used to support it, and the need for initiating reliability assurance as early in the design process as possible. This is because the sooner that potential design problems or vulnerabilities can be identified, the smaller the budget and schedule resources needed to correct them. It is much easier and less expensive to correct problems while the design is preliminary, than it is to correct them after the design has been finalized and equipment purchase or construction specifications have been issued. However, correction during this phase is still much less difficult, and less expensive, than if the problem is discovered after the equipment has been procured and installed in the field.

Reliability assurance not only tries to prevent or limit the costs of correction for unwanted design defects or weaknesses, but also to introduce a positive focus for the design team. It does this by providing early identification of systems structures and components whose reliability, availability or maintainability are important to the future reliable safe and economic operation of the plant. This means that in addition to ensuring that the plant is constructed to meet the plant specifications and all deterministic criteria reflected by regulations, codes and standards and "good" industrial practices, D-RAP ensures that the designer's attention is also focused on optimizing reliability and maintainability by improving it wherever it is both possible and justified. The RAP process also prevents the use of resources (budget and schedule) to achieve discretionary levels of reliability and maintainability which return life cycle benefits which are not commensurate with their costs.

There are several reasons for distinguishing between the RA programmes which will be applied during the design (D-RAP) and operational (O-RAP) phases of plant life, but, the most important is one of perspective. In the design and start-up process, each estimate of future plant economic performance and risk is "predictive", i.e. predictions of how well the new plant design will function throughout its life are derived from comparisons between the plant in design and other plants with documented operating experience, a complex inference process and the results from a range of analytical assessments and analyses.

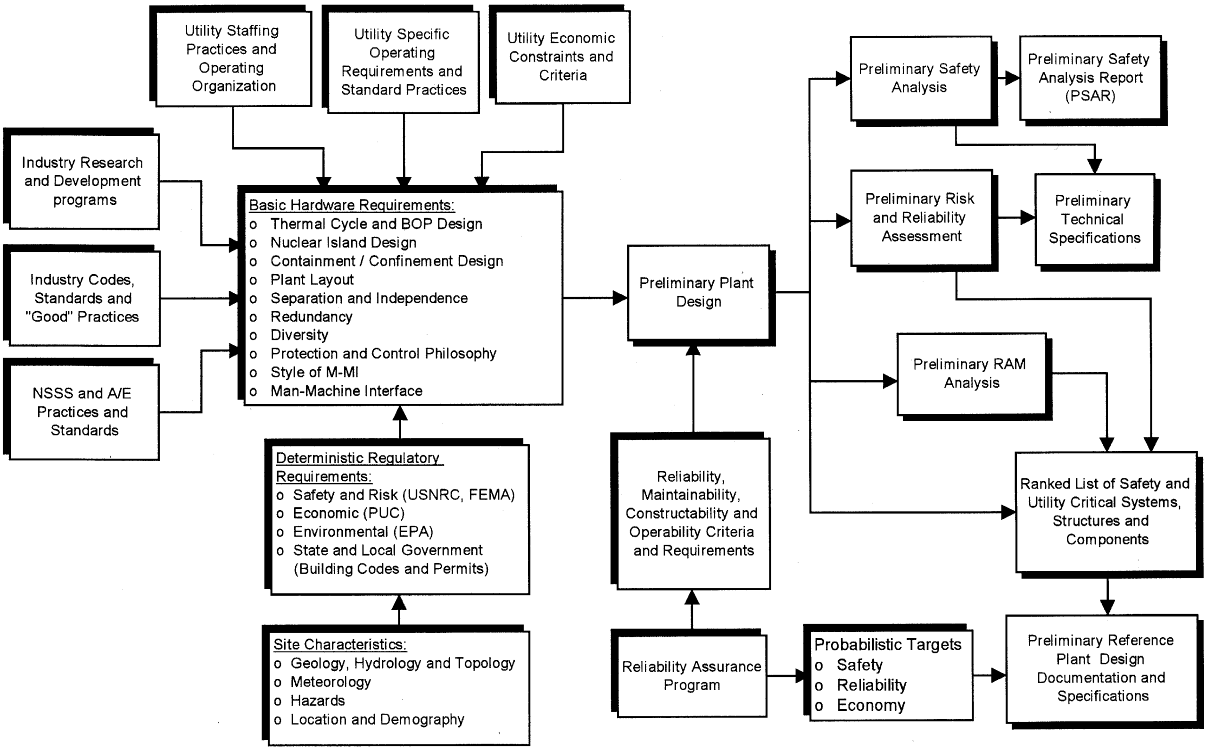
In an operating plant, collection of failure, repair and performance data slowly begins to provide a picture of the "plant specific character" of hardware and human performance. In the electrical generation processes, data taken from energy curtailments or maintenance budgets quickly show where hardware problems may lie. The re-occurrence of failures which RAP information identifies to be important contributors to lost revenue or increased operating costs can be prevented by effective root cause analysis. In this way, information from the operational RA programme is used to begin the process of "continuous improvement" which is inherent to all availability improvement programmes.

When SSC failures affect the expected frequency or consequences of severe accidents, the "safety" issues, differences between the applicable D-RA and O-RA programmes becomes less obvious. This is because, unlike generation systems whose failure is often manifest by an immediate reduction in plant output, the importance of a safety system failure or degraded condition may not be immediately apparent. The effects from the failure must be propagated, probabilistically, throughout the plant to determine its importance and the extent to which corrective or remedial measures should be initiated.

Though both D-RAP and O-RAP are functionally similar and have the same overall objectives, this difference in perspective between "prediction" and "retrospection" means that there are differences between the tools which must be used to achieve the desired results. As a consequence, although there is great deal of overlap between them, it is generally easier to describe each programme separately. It is important to view the reliability assurance programme as an overall guiding process which remains functionally unchanged throughout the life of the plant, but, adapts to the specific needs of the plant as it evolves from one phase to the next, i.e. from a concept to a fully functional operating nuclear generating facility.

## 3.2. RELIABILITY ASSURANCE DURING PRELIMINARY DESIGN

The overall D-RAP shown in Fig. 3-1 is further described by the process shown in Fig. 3-2. These diagrams depict the overall D-RA process, together with the iterative loops which are inherent to all processes in which optimization must be performed within a set of prescribed constraints. The diagram shows two separate loops, one for the "evolutionary" plant, the other for the "innovative" plant. The similarities and differences which exist within the RAP for each type will be described below.



Utility Staffing Practices and Operating Organization
Utility Specific Operating Requirements and Standard Practices
Utility Economic Constraints and Criteria
Industry Research and Development programs
Industry Codes, Standards and "Good" Practices
NSSS and A/E Practices and Standards
Basic Hardware Requirements:
o Thermal Cycle and BOP Design
o Nuclear Island Design
o Containment / Confinement Design
o Plant Layout
o Separation and Independence
o Redundancy
o Diversity
o Protection and Control Philosophy
o Style of M-MI
o Man-Machine Interface
Deterministic Regulatory Requirements:
o Safety and Risk (USNRC, FEMA)
o Economic (PUC)
o Environmental (EPA)
o State and Local Government (Building Codes and Permits)
Site Characteristics:
o Geology, Hydrology and Topology
o Meteorology
o Hazards
o Location and Demography
Preliminary Plant Design
Reliability, Maintainability, Constructability and Operability Criteria and Requirements
Reliability Assurance Program
Probabilistic Targets
o Safety
o Reliability
o Economy
Preliminary Safety Analysis
Preliminary Safety Analysis Report (PSAR)
Preliminary Risk and Reliability Assessment
Preliminary Technical Specifications
Preliminary RAM Analysis
Ranked List of Safety and Utility Critical Systems, Structures and Components
Preliminary Reference Plant Design Documentation and Specifications

*FIG. 3-1. Reliability assurance during preliminary ALWR design.*

### 3.2.1. The innovative plant

The innovative plant represents an advanced plant which incorporates radical conceptual changes in design approaches or system configuration in comparison with existing practice". Substantial R & D, feasibility tests, and a prototype or demonstration plant are probably required. The implication from this concept is that the designer of an innovative design should initiate some form of functional analysis of the reactor to ensure that all discrete critical functions and their hierarchy of sub-functions are clearly identified and understood before the success paths which can provide these needed functions are selected. Without this functional

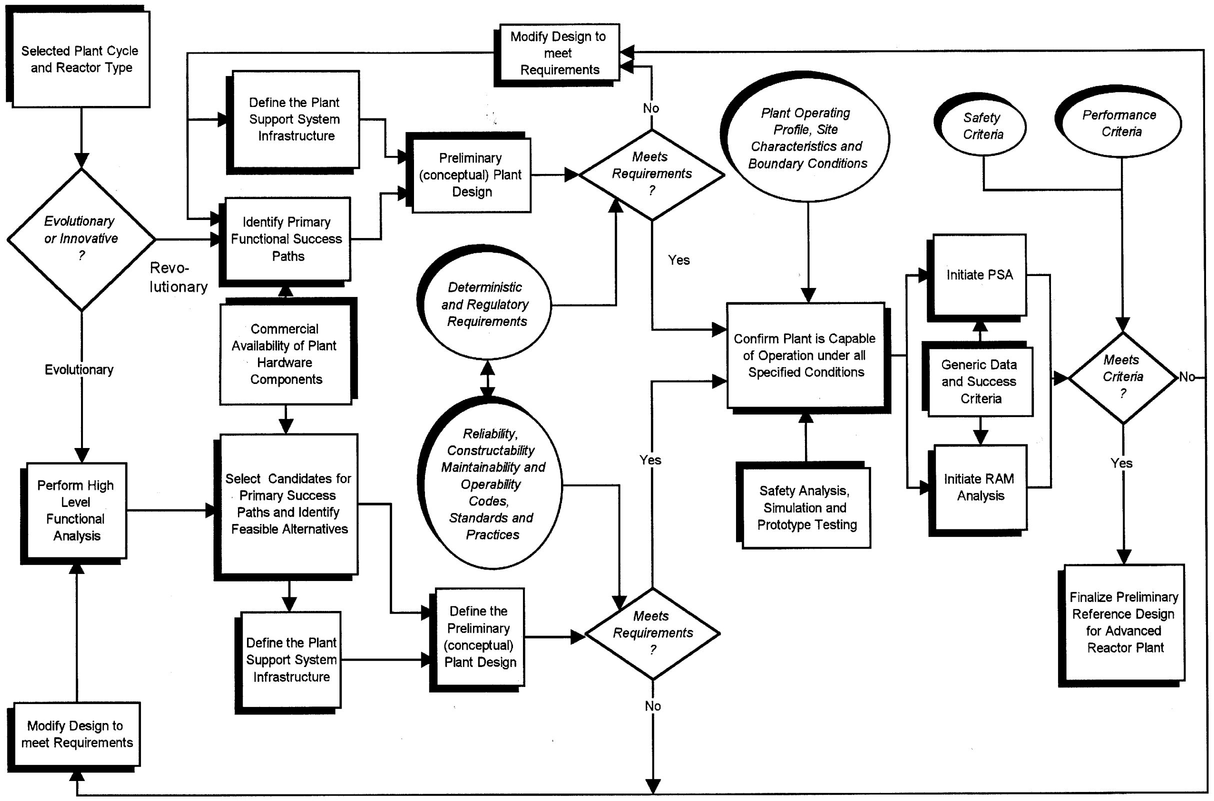

Selected Plant Cycle and Reactor Type
Evolutionary or Innovative ?
Revo- lutionary
Evolutionary
Define the Plant Support System Infrastructure
Identify Primary Functional Success Paths
Commercial Availability of Plant Hardware Components
Modify Design to meet Requirements
Preliminary (conceptual) Plant Design
No
Meets Requirements ?
Yes
Plant Operating Profile, Site Characteristics and Boundary Conditions
Safety Criteria
Performance Criteria
Deterministic and Regulatory Requirements
Reliability, Constructability Maintainability and Operability Codes, Standards and Practices
Initiate PSA
Confirm Plant is Capable of Operation under all Specified Conditions
Generic Data and Success Criteria
Meets Criteria ?
No
Yes
Perform High Level Functional Analysis
Select Candidates for Primary Success Paths and Identify Feasible Alternatives
Safety Analysis, Simulation and Prototype Testing
Initiate RAM Analysis
Yes
Finalize Preliminary Reference Design for Advanced Reactor Plant
Define the Preliminary (conceptual) Plant Design
Meets Requirements ?
Define the Plant Support System Infrastructure
No
Modify Design to meet Requirements

*FIG. 3-2. ALWR "Reliability assurance in design" (D-RAP).*

analysis and a clear definition of the functional requirements and objectives for each success path, the possibility always exists that important success paths may be omitted from the initial design, or more likely, selection of the success paths for the functions will be less than optimal, i.e. able to provide more than one function, and as a result fail to take advantage of options which either add reliability without an increase in cost, or result in a plant which meets all defined criteria with a lower overall cost. An effective overview of the functional analysis technique and how it can be used in the design process is described in the "Integrated Approach Methodology: A Handbook for Power Plant Assessment", issued by Sandia National Laboratories in 1987 (SAND87-138).

*Preliminary conceptual design for an innovative reactor design*

Following completion of the functional analysis, to whatever extent is necessary to fully augment the information provided by the reactor vendor or designer, the plant reliability structure will be developed. This preliminary design will provide clear definition of the operating critical functions, likely success paths and all failures in these success paths which initiate threats to the critical functions. These failure events will ultimately become the accident initiators for the PSA and the initiators of plant upsets which culminate in forced reductions or full forced outages.

Associated with these primary or "front line system" success paths is the entire plant support system infrastructure which provides motive power, control, actuation, cooling and inventory for systems, subsystems and components. The design of this support system network is developed to the sub-system or train level and then compared to all deterministic criteria to confirm that the fundamental design meets the basic requirements which will be imposed by regulatory agencies or defined by accepted industry codes, standards and good practices. This is also the point in the design process where the proposed plant layout should be reviewed to confirm that when the plant reliability infrastructure is superimposed upon the layout, all separation criteria are satisfied and that coupling between failure events induced by external threats to the plant are minimized, i.e. that there are barriers in place wherever unwanted inter- and intra-system interactions are prevented.

Strategies to defend against all forms of common cause failures and to avoid reliance on human actions to achieve critical functions must be implemented from the onset of the design process. This is because contributions from common cause failures and human error will likely dominate all other causes of overall safety system unreliability in the highly reliable plant design of the future. A rule of thumb indicates that as the probability of system failure decease below 1E-04, its failure probability will be increasingly dominated by all associated common cause failure probabilities.

The second item which is of great importance to the preliminary design is the incorporation of reliability, constructability, maintainability and operability standards. These are typically described by the user's requirements documents developed by individual member states to provide an overall blanket assurance that the fundamental design decisions consider their effects on plant reliability, availability and safety.

### 3.2.2. The evolutionary plant

The evolutionary plant is an advanced design that achieves improvements over existing plants through small to moderate modifications, with a strong emphasis on maintaining design proveness to minimize technological risks. The development of an evolutionary design requires at most engineering and confirmatory testing.

Because it has been derived from an earlier successful design, in many respects the evolutionary reactor plant design can be expected to exhibit a great deal of similarity to existing reactors. Plant-to-plant layout may vary to accommodate individual site characteristics or to incorporate changes which come from insights and lessons learned from construction and operation of its predecessors.

The implication from having these similarities likely means that the impetus for performance of a comprehensive plant functional analysis may be reduced and that the basic design parameters which will define the overall plant reliability structure are already well characterized. In which case, the first step in the design process may involve development of the "master plant logic diagram" (MPLD, see Section 5.17.1.1) and superimposition of the proposed plant layout site to confirm that the overall broad design concept meets all applicable deterministic criteria, established by either the regulatory agencies or by the owner/operator to reflect industry standards, codes and commitments and the deterministic criteria defined in the URDs.

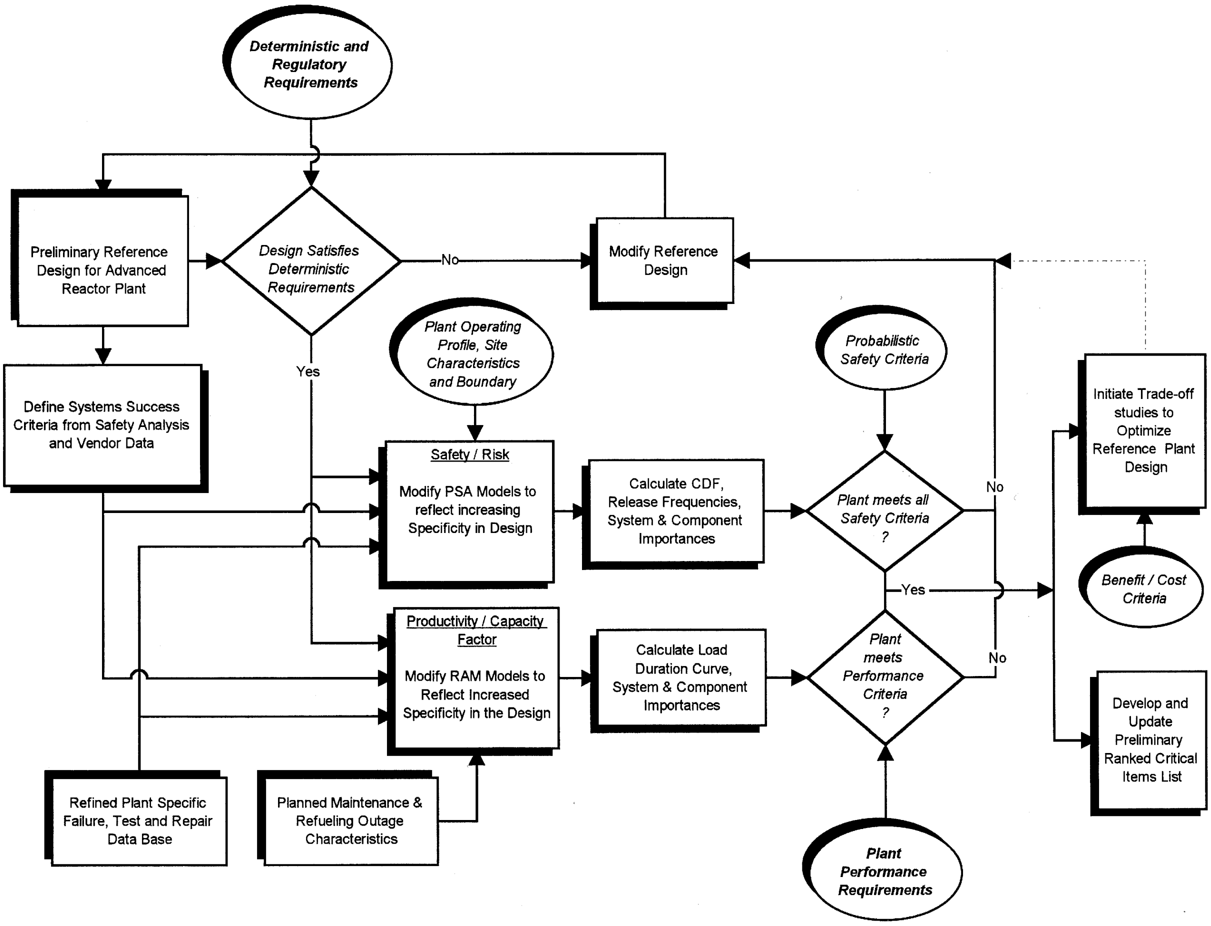
Wherever discrepancies arise, the design must be modified to meet the overall requirements, and the MPLD (or other equivalent tool) and plant layout revisited to confirm that the modified design meets the defined criteria and that changes did not introduce new problems which could affect the reliability of any plant functions.

After completion of the preliminary design for either the evolutionary or innovative reactor plants, the RAP process becomes similar. The only expected differences between the RA programmes for each reactor plant class are expected to come from the need for analytical tools and methods which have necessary computational and simulation capabilities to support the RAP decision making process. For example, the analytical tools and methods needed to perform the safety analysis and confirm the capability of the design for the evolutionary reactor, may be less effective for use in the safety analysis for the innovative design, which likely will exploit passive systems to a much greater extent.

Computer codes used to predict the effects from loss of forced primary system flow may not be much less capable of demonstrating the effectiveness of cooling systems which use natural circulation and rely on relatively small driving heads. Similarly, the reliability of conventional active hardware systems can be predicted with a great deal of confidence, but the mechanisms of failure for passive systems may be so different that there may be a great deal of uncertainty associated with the predictions. This will have an effect on the tools and methods used in the PSA for each reactor class. However, the functional objectives for these analyses are identical, so programmatically, there will be little difference between RAP for each reactor class.

## 3.3. D-RAP OPTIMIZATION DURING PRELIMINARY DESIGN

Fig. 3-3 provides an overall diagrammatic representation of how a RA programme can be used in the optimization of the preliminary generating plant design process for both evolutionary and innovative plant designs. Within this process, there is an implicit assumption that the preliminary design has already been reviewed to confirm that it complies with all deterministic criteria and requirements imposed by regulatory agencies, industry oversight groups and utility organizations, and that any changes to the design which are needed to meet these requirements have already been implemented.



Deterministic and Regulatory Requirements
Preliminary Reference Design for Advanced Reactor Plant
Design Satisfies Deterministic Requirements
No
Modify Reference Design
Yes
Define Systems Success Criteria from Safety Analysis and Vendor Data
Plant Operating Profile, Site Characteristics and Boundary
Probabilistic Safety Criteria
Safety / Risk
Modify PSA Models to reflect increasing Specificity in Design
Calculate CDF, Release Frequencies, System & Component Importances
Plant meets all Safety Criteria ?
No
Initiate Trade-off studies to Optimize Reference Plant Design
Yes
Benefit / Cost Criteria
Productivity / Capacity Factor
Modify RAM Models to Reflect Increased Specificity in the Design
Calculate Load Duration Curve, System & Component Importances
Plant meets Performance Criteria ?
No
Develop and Update Preliminary Ranked Critical Items List
Refined Plant Specific Failure, Test and Repair Data Base
Planned Maintenance & Refueling Outage Characteristics
Plant Performance Requirements

*FIG. 3-3. D-RAP — Overview of the optimization process.*

The four steps described below typify those which necessarily must be taken to confirm that the preliminary design can be expected to meet each of the prescribed probabilistic performance and safety goals. These steps should be completed before initiating the final detailed design process so that any needed changes in the basic design philosophy can be made before existing schedule commitments make correction of changes excessively expensive.

(1) Confirm that the design is capable of withstanding all important or expected threats to the plant critical protective functions, under a clearly defined set of boundary conditions, without resulting in failure of the fuel clad or failure of the primary containment. This analysis is conventionally called the "safety analysis". This analysis proceeds on the basis of an assumed set of predefined hardware and support systems failures and associated plant conditions which define the boundary conditions for the analysis. the analysts use thermal hydraulic simulation techniques, modeling or prototypical testing to confirm that the "as designed" safety systems are capable of maintaining the reactivity and heat removal functions which are necessary to prevent failure of the fuel clad, primary circuit and containment barriers to fission product release.

The boundary conditions assumed during the safety analysis and the results and plant conditions they represent are initially documented in the preliminary safety analysis report (PSAR or equivalent nomenclature).

The validity of the documented assumptions used in the performance of the safety analysis must be maintained during plant operation so they are clearly identified and incorporated into the bases for the preliminary plant technical specifications. In fact, this publication becomes the repository for all conditions within which the plant must operate to ensure that the safety envelope assumed in the licensing process remains intact throughout the life of the plant.

(2) Confirm that the design can be expected to meet all prescribed economic performance measures, which include equivalent availability, full and partial forced outage rates, planned outage rates and capacity factor.

The reliability, availability and maintainability (RAM) analysis assesses the expected contribution to loss of capacity factor from each individual potential contributor, typically:

- Equivalent unavailability of the systems which must function during the electric generation process during power operation,
- Reliability of each system whose failure results in a plant SCRAM and the expected SCRAM (reactor/turbine trip) rate,
- Average down times which are expected to follow the important causes of plant SCRAMS and estimates of the expected plant full forced outage rate,
- Maintenance and test requirements which are likely to dominate the contributions to lost generation from planned outages.

A case study describing an application of some of the analytical approaches which are available for performance of plant-wide RAM analyses during the design process is provided in Annex A-3 of this guidebook.

(3) Confirm that the design is balanced, i.e. exhibits a flat risk profile in which the magnitudes of the important individual functional contributors to risk are similar, and that the overall design is expected to meet all prescribed probabilistic safety criteria. These criteria may include core damage frequency (CDF), frequency of a large release of fission products and the individual risk for members of the public living near the plant.

Confirmation that the plant can be expected to meet these defined goals will be done by building and quantifying a preliminary plant risk/safety assessment. The PSA will be built from the most complete set of available design and analytical information. This is expected to include:

- Transient initiating events and their expected frequencies from the plant reliability analysis,
- External initiating events from the environmental threats identified during the site selection and preliminary assessment activities,
- Plant functional response to the set of identified initiating events,
- The expected primary system success paths and plant support system infrastructure, detailed to the train or sub-system level,
- Systems success criteria derived from the safety analysis,
- Sufficient detail to identify all important contributors from human error and common cause failures,
- A failure and repair database which is appropriate to the plant, but, likely derived from generic sources,
- Information and insights taken from other completed PSAs which are applicable to the new plant design,
- Containment functional behaviour from prototypical testing, the safety analysis or other severe accident studies or simulations,
- The area demography throughout the expected plant life-time.

The results from the analysis will provide a “first look” at the likelihood that the plant will meet all of the defined probabilistic criteria and also provide an indication of the areas which are important to the overall management of plant risk. It is particularly important for the PSA to identify all important human actions and potential common cause failures early in the design so that strategies to prevent them or minimize their impact can be implemented during detailed plant design.

As the results of these analyses are compared with the defined plant performance criteria, where enhancement is needed, the design will be modified, where no further changes are needed the preliminary design will be defined as the “reference design”, or the point of reference from which all future assessments and design changes will evolve.

(4) Confirm that the design can be expected to meet all prescribed deterministic criteria established by both regulatory and commercial (owner/operator) entities.

Within the scope of this functional activity, the preliminary plant reference design will be carefully reviewed to confirm that the plant continues to meet all deterministic criteria and requirements. This is particularly important when feedback from the results of the PSA or RAM analysis have been used to optimize the design, i.e. resulted in plant configuration changes after the original deterministic assessment had been completed.

## 3.4. RELIABILITY ASSURANCE DURING FINAL DESIGN

After the initial assessment of the reference design and confirmation that the plant can meet all of the prescribed criteria, the final design process moves into full swing. The role of the RA programme during final design is similar to that used in the preliminary design process, except that it is used much more actively to focus the design on the enhancement of reliability, availability and maintainability in each important area, and to serve to cost-efficient design change so that it is optimized to the maximum extent possible.

The RAM and PSA models are updated and increased in explicit detail as the design matures and the available information for the success paths use for both power generation and safety systems becomes better defined.

Many methods for reliability and availability analyses, and the optimum approach must be selected for each specific application and frequently differ in both implicit and explicit levels of detail. As the RAM and PSA models evolve to match the characteristics of the maturing design, changes in modeling technique, methods, codes and databases are often required. The following provides some insight into this particular aspect of RAM and PSA modeling when it is used throughout the design process to demonstrate that the design meets or exceeds the prescribed availability or reliability goals and to identify those components which represent important vulnerabilities or likely sources of future generation losses.

The process of updating the reliability, availability and safety models parallels the design in the manner described in Section 2 and described by Fig. 2-7. RAP is used in the final design process to guide the designers by providing the necessary feedback to indicate which parts of the design are expected to dominate the risk or capacity factor and to establish the worth of any changes which may be proposed to reduce their importance. The results from the analysis should be fed back as a set of importances which are ascribed to individual systems structures and components. This ranked list will evolve throughout the final design process and culminate in the identification of the hardware for which specific reliability and maintainability criteria should be established by the procurement specifications.

The RAM and PSA models will include all human actions which are important either to the overall management of the plant or to the operator's ability to influence the reliability or availability of important plant systems, either by because these actions preventing or assist in the recovery from plant SCRAMs or the failure of safety systems used in the prevention and management of severe accidents. The result from the solution and quantification of the analytical models serve to provide a basis for assessment of the information presented to the plant operating staff and to confirm that it is adequate for effective decision making during the performance of these important human actions.

The results from the RAM and PSA studies for the final design will culminate in the identification of a critical items list which represents all systems, structures and components which are ranked in order of their importance to both generation and safety, the areas of importance to the overall risk or capacity factor of the plant and confirmation that both the performance and safety goals for the plant are likely to be met by the proposed design. These results will be used to guide the overall optimization for the plant and focus resources on achieving optimal levels reliability and maintainability for important components during the specification, evaluation and selection of components in the procurement process and to establish maintainability criteria for the layout and construction of these same components.

## 3.5. ELEMENTS OF DESIGN RELIABILITY ASSURANCE (D-RA)

### 3.5.1. Assignment of system reliability and availability goals

Because the optimization process is expected to be resource and schedule intensive, identification of areas of the design which potentially merit attention is one of the first steps. This information will be provided by the list of SSCs, which is ranked on the basis of both importance to safety and to capacity factor, and the application of a screening criterion, i.e. a limiting value of importance where commercially available hardware is expected to provide acceptable performance. The single exception could result from systems whose importance is low because of high levels of redundancy. In which case, systems should be reassessed in the manner suggested by Fig. 3-4.

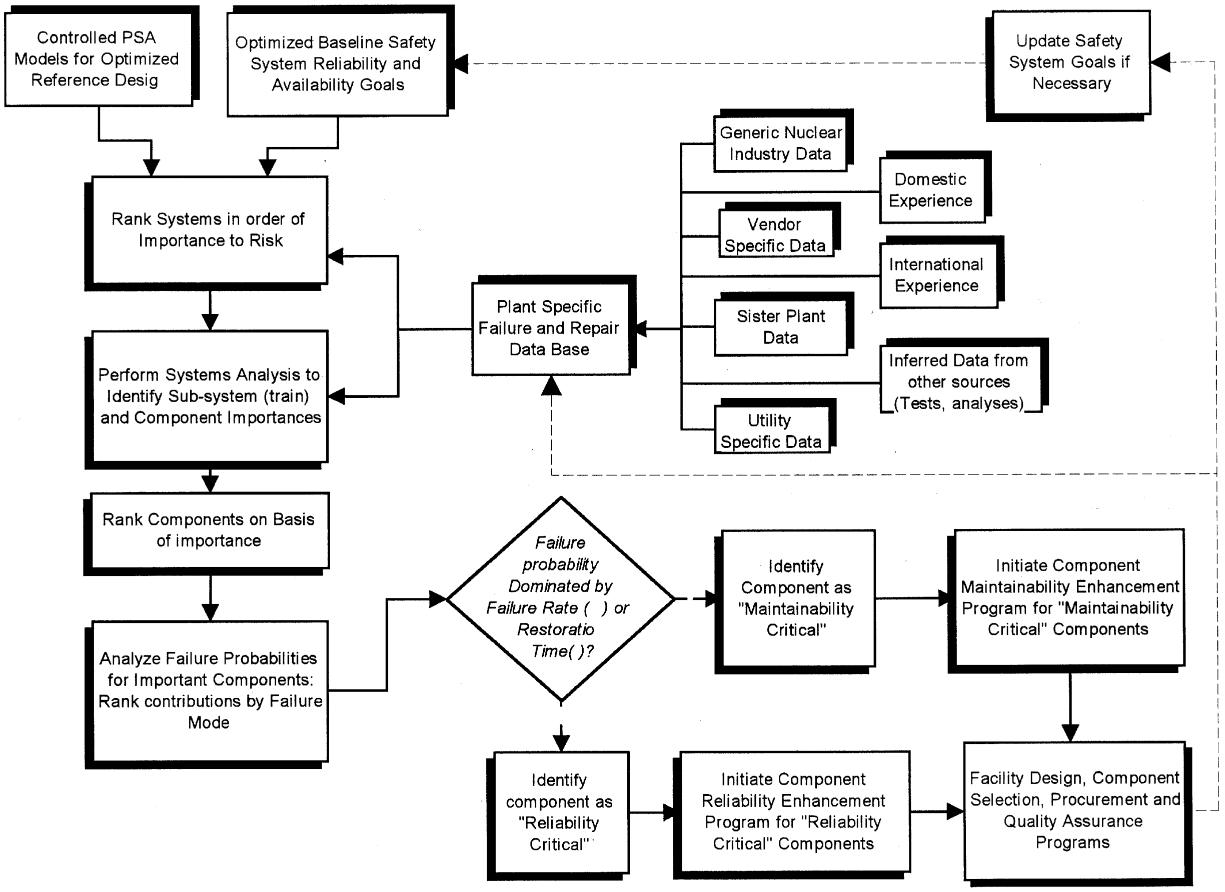

Controlled PSA Models for Optimized Reference Desig
Optimized Baseline Safety System Reliability and Availability Goals
Update Safety System Goals if Necessary
Rank Systems in order of Importance to Risk
Generic Nuclear Industry Data
Domestic Experience
Vendor Specific Data
International Experience
Plant Specific Failure and Repair Data Base
Sister Plant Data
Inferred Data from other sources (Tests, analyses)
Perform Systems Analysis to Identify Sub-system (train) and Component Importances
Utility Specific Data
Rank Components on Basis of importance
Failure probability Dominated by Failure Rate ( ) or Restoratio Time( )?
Identify Component as "Maintainability Critical"
Initiate Component Maintainability Enhancement Program for "Maintainability Critical" Components
Analyze Failure Probabilities for Important Components: Rank contributions by Failure Mode
Identify component as "Reliability Critical"
Initiate Component Reliability Enhancement Program for "Reliability Critical" Components
Facility Design, Component Selection, Procurement and Quality Assurance Programs

*FIG 3-4. D-RAP — Critical component and system identification.*

The ranked list of SSCs, which represents the systems, structures and components whose reliability or availability is important to electricity generation or safety, and the extant system reliabilities and availabilities which are predicted by the “best estimate” RAM and PSA analyses are used as the basis for the allocation process. The list is subdivided into segments, within which individual SCCs can be categorized as having “High, Medium or Low” importance. The actual segregation criteria must be developed on the basis of the expected relationships between importance measures and their corresponding relationship to economic importance. Segregation into groups is done to provide a more efficient approach towards the optimization and trade-off process and a basis for prescreening before individual quantitative assessments are made with the PSA and RAM models.

When systems exhibit high levels of importance because there is little or no functional redundancy, indicated by its Birnbaum importance measure, the design team should consider:

> *Adding redundancy or diversity in the form of additional systems, trains, or sub-systems or a formulate changes to the support system infrastructure to maximize the functional independence between important functional success paths.*

If redundancy changes are not warranted, i.e. lack of redundancy is not the reason for high importance, or, increases in redundancy are not economically warranted, then the design team should consider:

> *Placing the hardware in a category whose procurement specifications are written to assure that it is purchased for high reliability and, or, high maintainability.*

If safety system trains or major components exhibit **low** levels of predicted importance, the design team should consider whether or not it is the result of excessive redundancy and whether a reduction in redundancy can be considered to reduce cost. The SSC evaluation process may also indicate where it may be possible to reduce plant capital cost by replacing commercially available equipment with higher cost, reliability, or maintainability assured equipment and as a consequence, reduce redundancy.

Each design decision must be constrained by the deterministic requirements imposed by regulatory codes and standards and whether the plant's "as-designed" levels of redundancy allow traditionally time directed planned maintenance to be performed on-line so that any increased costs from providing redundancy are compensated by a corresponding reduction in planned outage costs.

Systems with medium importance must be reviewed from each of the above perspectives to determine whether a premium should be paid for individual SSCs which have higher quality and reliability in order to minimize the need for redundancy, or whether the use of commercially available components will be adequate.

In the last remaining step in the optimization process, the designer uses a series of sensitivity studies to examine the reliability/availability/cost gradients and identify areas where plant risk can be maintained at a constant level while reallocating reliability and availability goals between high importance systems with those of low or medium importance, i.e. determine whether overall plant capital and operating costs can be reduced by accepting lower reliability or maintainability in a high cost system while compensating for its effects on risk by increasing the reliability or maintainability in other systems, where the improvement can be achieved at a lower cost.

Reallocation of system goals should always be considered if:

- An identified reallocation strategy will produce an overall reduction in life cycle plant costs (capital plus operating and maintenance costs), and,
- The design remains risk neutral, i.e. the net effect on risk from the reallocation of reliability or availability goal contributions from one system to another is zero.

At the conclusion of the optimization and reallocation process, the RAM and PSA system models will be re-solved in their final configurations and the resultant predictions of system availability and reliability levels will become the basis for future performance measuring criteria and goals.

It is essential that, at the conclusion of the optimization process, each defined SSC reliability and availability goals is both practical and feasible, and that the underlying analyses use best estimate, high confidence, values provided by the future plant maintainers and the equipment vendors. Specific elements of this System goal Allocation and Optimization Process are described in more detail below.

#### *3.5.1.1. Redundancy in system design*

If only a single train is mandated by the deterministic design acceptance criteria, any decisions to increase the levels of redundancy should come from an assessment which shows that a single train design is inadequate to meet the plant functional needs throughout its operating spectrum. The effects of maintenance are a particular concern for a single train system, and whether the plant is placed in a vulnerable position during on-line maintenance, either because the resulting configuration increases the likelihood of SCRAM, reduction in capability or increases the probability of failure of a specific safety function to an unacceptable level.

If the reduction in redundancy has no prohibitive effects, then the question comes up as to the benefit of doing so, and how the assessment of benefits should proceed. Figure 3-4 highlights suggests the process elements needed to perform the benefit assessment.

### 3.5.2. Cost/benefit assessment

The designer must assess and optimize the change in safety/risk or change in capacity factor which will result from the proposed change in redundancy or component reliability. This will be achieved with the modification and requantification of either the PSA or RAM models or their results. The selected approach will depend very much upon the nature of the proposed change and the functional effects that follow. The following examples typify the general issues associated with the process and viable quantitative approaches:

- If the change affects both SCRAM rate and capacity factor, the expected benefits are quantified with the RAM (reliability) models and the results from the analysis used to modify the input data (initiating event frequency) for the PSA to find any additional impacts attributable to a change in plant risk;
- When the change affects only the reliability or availability of a safety system, the PSA will be used to quantify the magnitude of its expected benefits;
- RAM and/or PSA models will be used to quantify any changes in CDF, LERF, risk, capacity factor, FOR, or SCRAM frequency which can be expected from the baseline “pre-modification” and “post-modification” plant configurations. Comparison of these results will measure the benefits from changes in plant safety and production which are directly attributable to the proposed modification;
- The expected life cycle equivalent present worth of the predicted benefits will be calculated from either a detailed economic risk assessment or from a set of simpler economic models which use surrogate economic measures to substitute for actual calculated costs;
- The cost of each proposed modification will be measured in terms of the equivalent present worth for its aggregate life cycle implementation, i.e. any repeated costs which occur throughout the life of the plant which are attributable to the modification will be capitalized and added to the procurement and installation costs;

- Repeated costs originate with expected or required maintenance and overhaul strategies, or any other additional costs which can be attributed to the change;
- A comparison between the expected costs and benefits which are directly attributable to the change will be used to guide any implementation decisions.

### 3.5.3. Prioritization of candidate design improvements

Where to begin and how to prioritize issues so that they become candidates for design optimization is an important issue in the general optimization process. The first step, for both safety/risk and productivity issues, involves the use of the critical items list to focus the optimization process. A process for developing this rank ordered list of SSCs is provided graphically by Fig. 3-3, which in turn is followed by Fig. 3-4–3-7. These figures depict possible processes which can be used to identify critical plant components and systems, optimize trade-off analyses for both safety and generation systems, and allocate system level goals.

A general rule of thumb indicates that if a system, structure or component is important to risk or productivity, its potentially high marginal value represents a fertile area for optimization and the possibility of enhancement at an attractive cost. Another way of saying this, is that:

- SSC’s with high levels of importance imply a potentially large budget for positive change,
- An SSC with low importance is likely to have an implicitly small budget to support change.

This is not meant to imply that SSCs with low importance will be ignored and dropped from the list. Eventually, the potential for change in each SSC will be examined, because, although SSCs may exhibit low importance, there may still be opportunities for cost effective enhancement. The focus of activities intended to enhance the performance of these low importance components is likely to be limited to procedural, administrative or informational improvements, sometimes referred to as “software”, i.e. “non-hardware”, improvements. This is because implementation costs for these types of changes are generally much lower than the costs of implementing hardware changes, so they are much more likely to be cost effective. For example:

- If a SSC has “low” importance, a search for improvement should probably focus on “software changes”;
- If the SSC has “high” importance, the additional benefits from an increase in its reliability may justify a search for capital “hardware” improvements, in addition to the search for “software” improvements.

When the candidate list of SSCs has been identified, the next steps in the process involve an assessment of their individual improvement potentials, and where improvements are deemed possible, an assessment of the implementation costs for each improvement strategy.

The RAP optimization programme attempts to develop the relationship between the incremental cost of achieving improved life cycle reliability and productivity and the incremental life cycle benefits which result from this increased reliability or availability. If this ratio can be determined, then the optimization process can be initiated so that the maximum improvement is achieved for minimum cost. Because this is a complex issue, the initial optimization will be undertaken at the system and sub-system level, and only after all train level decisions have been made, will the focus move to individual components.

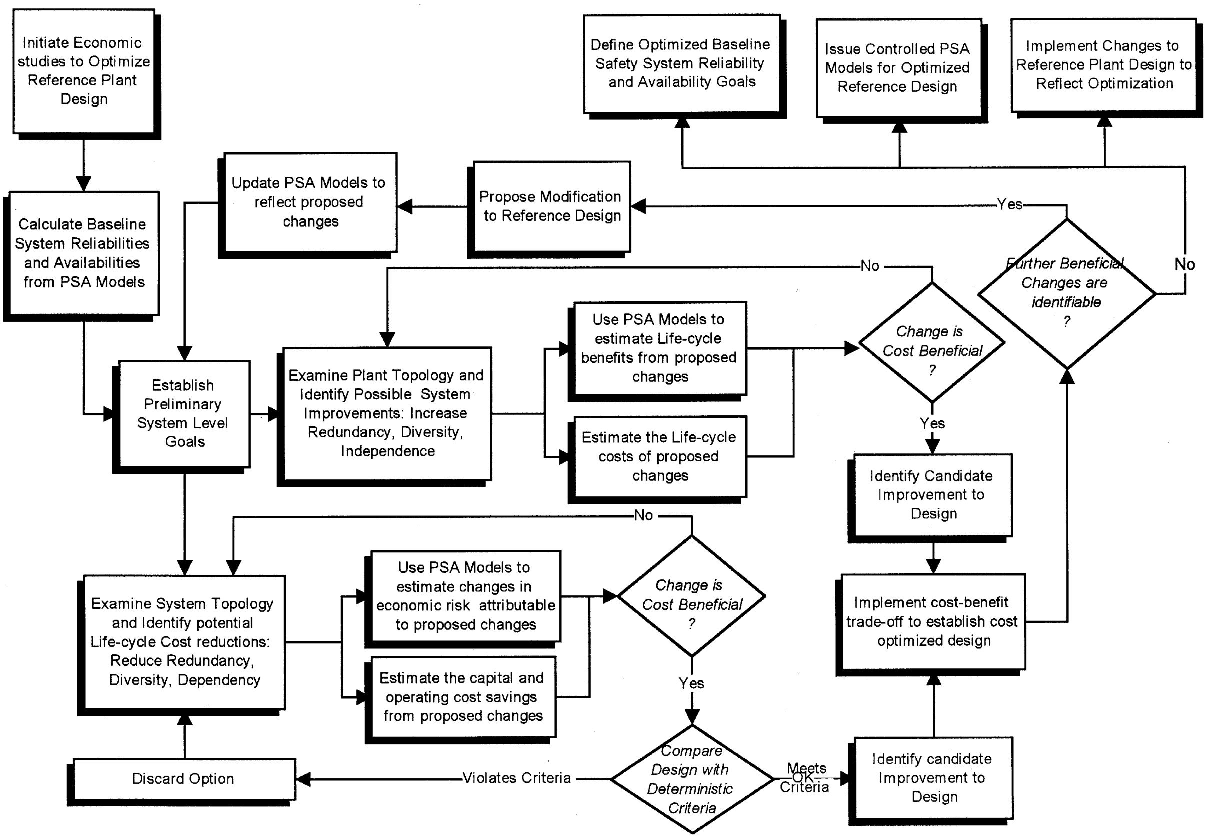

Initiate Economic studies to Optimize Reference Plant Design
Define Optimized Baseline Safety System Reliability and Availability Goals
Issue Controlled PSA Models for Optimized Reference Design
Implement Changes to Reference Plant Design to Reflect Optimization
Calculate Baseline System Reliabilities and Availabilities from PSA Models
Update PSA Models to reflect proposed changes
Propose Modification to Reference Design
Yes
No
Further Beneficial Changes are identifiable ?
No
Use PSA Models to estimate Life-cycle benefits from proposed changes
Change is Cost Beneficial ?
Establish Preliminary System Level Goals
Examine Plant Topology and Identify Possible System Improvements: Increase Redundancy, Diversity, Independence
Estimate the Life-cycle costs of proposed changes
Yes
Identify Candidate Improvement to Design
No
Use PSA Models to estimate changes in economic risk attributable to proposed changes
Change is Cost Beneficial ?
Implement cost-benefit trade-off to establish cost optimized design
Examine System Topology and Identify potential Life-cycle Cost reductions: Reduce Redundancy, Diversity, Dependency
Estimate the capital and operating cost savings from proposed changes
Yes
Compare Design with Deterministic Criteria
Meets OK Criteria
Identify candidate Improvement to Design
Discard Option
Violates Criteria

*FIG. 3-5. D-RAP Ssafety system optimization.*

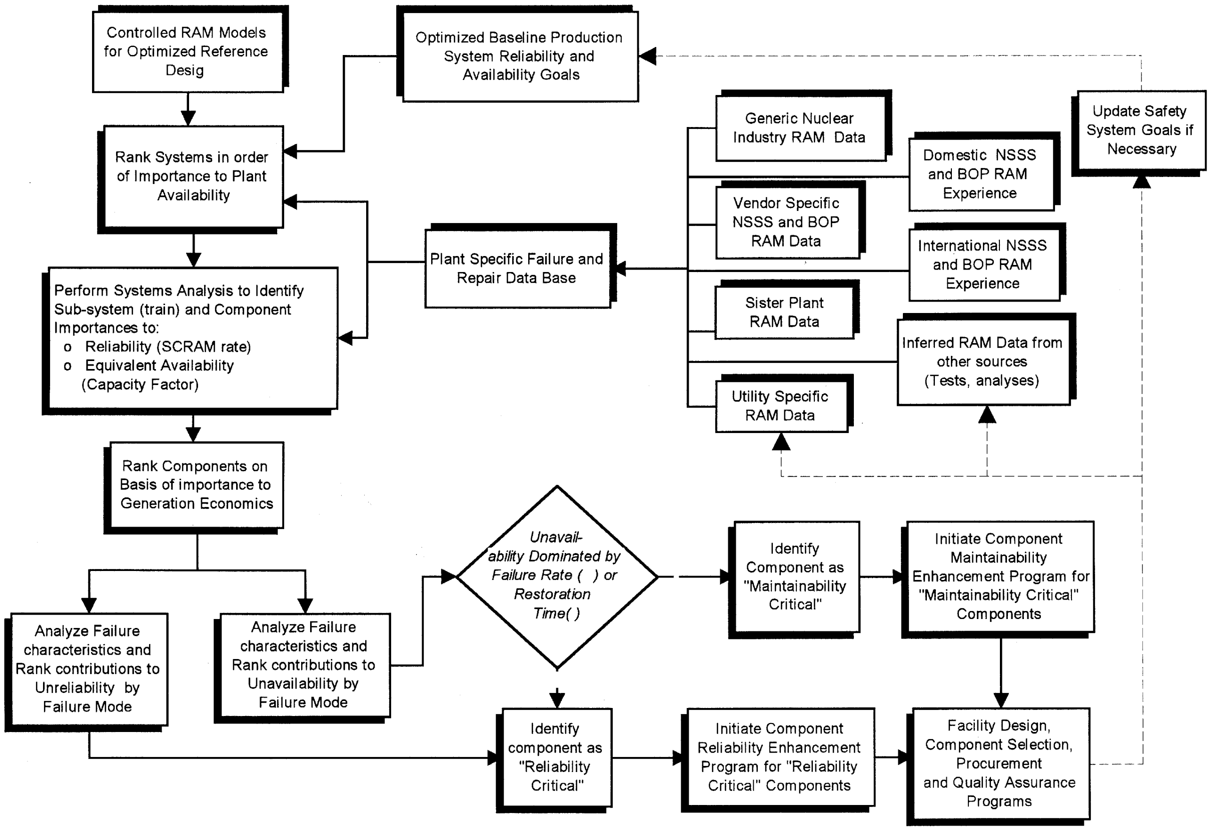

Controlled RAM Models for Optimized Reference Desig
Optimized Baseline Production System Reliability and Availability Goals
Rank Systems in order of Importance to Plant Availability
Generic Nuclear Industry RAM Data
Domestic NSSS and BOP RAM Experience
Update Safety System Goals if Necessary
Vendor Specific NSSS and BOP RAM Data
Plant Specific Failure and Repair Data Base
International NSSS and BOP RAM Experience
Perform Systems Analysis to Identify Sub-system (train) and Component Importances to:
o Reliability (SCRAM rate)
o Equivalent Availability (Capacity Factor)
Sister Plant RAM Data
Inferred RAM Data from other sources (Tests, analyses)
Utility Specific RAM Data
Rank Components on Basis of importance to Generation Economics
Unavail-ability Dominated by Failure Rate ( ) or Restoration Time( )
Identify Component as "Maintainability Critical"
Initiate Component Maintainability Enhancement Program for "Maintainability Critical" Components
Analyze Failure characteristics and Rank contributions to Unreliability by Failure Mode
Analyze Failure characteristics and Rank contributions to Unavailability by Failure Mode
Identify component as "Reliability Critical"
Initiate Component Reliability Enhancement Program for "Reliability Critical" Components
Facility Design, Component Selection, Procurement and Quality Assurance Programs

*FIG. 3-6. D-RAP-generation systems optimization*

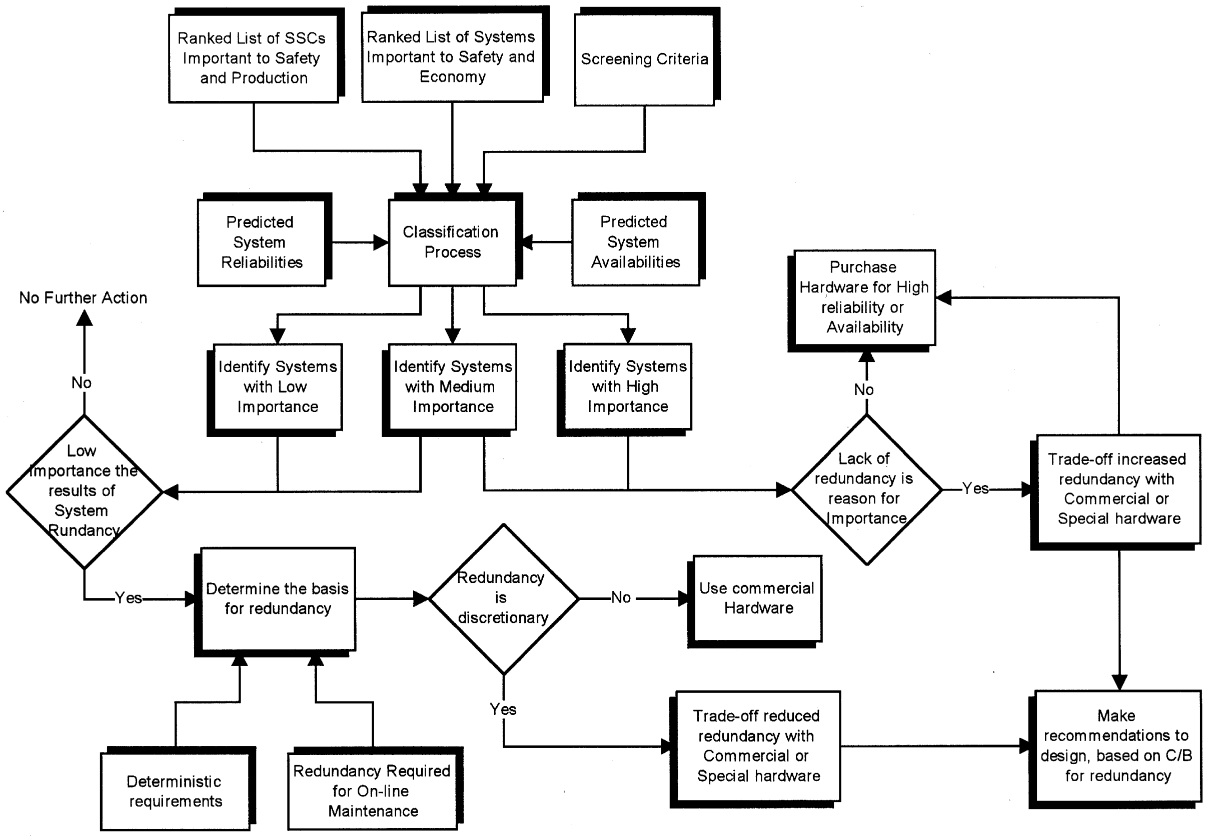

Ranked List of SSCs Important to Safety and Production
Ranked List of Systems Important to Safety and Economy
Screening Criteria
Predicted System Reliabilities
Classification Process
Predicted System Availabilities
Purchase Hardware for High reliability or Availability
No Further Action
No
Identify Systems with Low Importance
Identify Systems with Medium Importance
Identify Systems with High Importance
No
Low Importance the results of System Rundancy
Lack of redundancy is reason for Importance
Yes
Trade-off increased redundancy with Commercial or Special hardware
Yes
Determine the basis for redundancy
Redundancy is discretionary
No
Use commercial Hardware
Yes
Trade-off reduced redundancy with Commercial or Special hardware
Make recommendations to design, based on C/B for redundancy
Deterministic requirements
Redundancy Required for On-line Maintenance

*FIG. 3-7. System goal allocation optimization.*

It should be noted, that throughout the optimization process, the design will be continuously compared to all prescribed deterministic and probabilistic criteria, and at any time that a proposed design change results in violation of these criteria, it can immediately be withdrawn.

The safety analysis will be updated throughout this period whenever changes which effect the assumptions or boundary conditions are contemplated, and if the change affects system success criteria this information will be fed back into the PSA and productivity models.

Following system and sub-system optimization the process will continue to the component level. At this more detailed level, the approach may, however, take on a different character. At the point of completion of the train/system level optimization process:

- Each system will have a defined structure and an associated expectation of reliability,
- The quantitative levels of expected reliability and availability will be assigned to be the system goals,
- The more detailed optimization and design decision making activities will follow as the focus of the designers moves onto the final details and component selection and design,
- The system level RAM and PSA models will provide individual intra system component importances which correlate to, or support, the overall ranked list of SSCs.

The system and plant level component importances will be used to focus attention of the need to identify reliability, availability or maintainability criteria in the procurement and construction phases of plant life. SSC importance measures will be used to guide the application of all plant reliability or maintainability centered programmes throughout its operational life.

### 3.5.4. Results from optimization

At the conclusion of the design optimization phase, several products can be expected:

- A finalized reference design which can be used to initiate the specification, procurement and construction of plant hardware, associated with this will be:
  - (i) A set of probabilistic system performance goals to guide future plant performance requirements,
  - (ii) A ranked set of important systems, structures and components whose importance is traceable to the effects of their reliability, availability and maintainability on risk or on plant capacity factor.
- A set of RAM models and PSA models which accurately reflect the final reference design and the success criteria which have been derived from the safety analysis.

  Note:
  The PSA is a "best estimate analysis", i.e. uses the most realistic assumptions possible, whereas the deterministic safety analysis may use more conservative criteria to accommodate uncertainties in the behavior or performance of individual plant success paths and uncertainties in the effects from physical phenomena and their impact on the response of passive structures during severe accidents. The PSA provides explicit estimates of uncertainty.

  The differences in focus and individual issues between the PSA and the safety analysis may result in differences in the success criteria used in each of these analyses. This is acceptable, provided there is a documented, technically sound analytical basis for these differences, particularly in the use of less conservative success criteria in the PSA.

## 3.6. PLANNED OUTAGE RATES AND DESIGN OPTIMIZATION

To this point in the RAP process, the design has been guided by insights provided by results from the RAM and PSA analyses:

- SCRAM rates and transient initiating event frequencies, predicted by a plant reliability model,
- Equivalent availability predicted by a multi-state availability model,
- Forced outage rates predicted from each SCRAM or forced shutdown scenario, its frequency and the expected time to restore the plant to power operation,
- Core damage frequency, release frequencies and associated source terms and risks predicted by the PSA,
- A ranked list of SSCs where the order of each SSC is derived from its individual importance to overall risk, reliability and capacity factor,
- Individual system and sub-system availability and reliability goals, which (initially) represents their expected performance.

Optimization of outage times for important SSCs becomes the next goal for RAP. This ensures that the maintainability, testability and inspectability of components which are subject to surveillance or overhaul during planned outages supports a minimum outage length, and that refueling process equipment supports the expected planned outage rate goals.

To minimize contributions to unavailability from refueling and planned maintenance outages, a form of simulation is required to identify the items which are expected to be on the schedule critical path. This alone provides one important measure of their economic importance. Further examination of the required maintenance activities and their expected duration will provide additional support for assessing importance because the longer they remain on the critical path, the greater their economic impact.

The simulated preliminary outage schedule can be synthesized from known test and maintenance activities which are mandated by the cognizant regulatory body, recommended by the original equipment manufacturer (OEM) and an operability assessment to determine what maintenance can, or cannot, be performed on-line, i.e. at power.

Optimization of planned refueling and maintenance outages also depends upon whether or not, specific planned outage activities can result in the plant's being placed in a risk significant configuration. This leads to the need for a plant specific PSA which is performed specifically for the shutdown mode of operation. The results from the shutdown PSA and a ranked list of components and systems which are important to shutdown risk and whose maintainability and reliability must be maximized during the outage or during transitions to, and from, full power.

A flow chart detailing one possible overall process for optimization of planned outages is provided in Fig. 3-8.

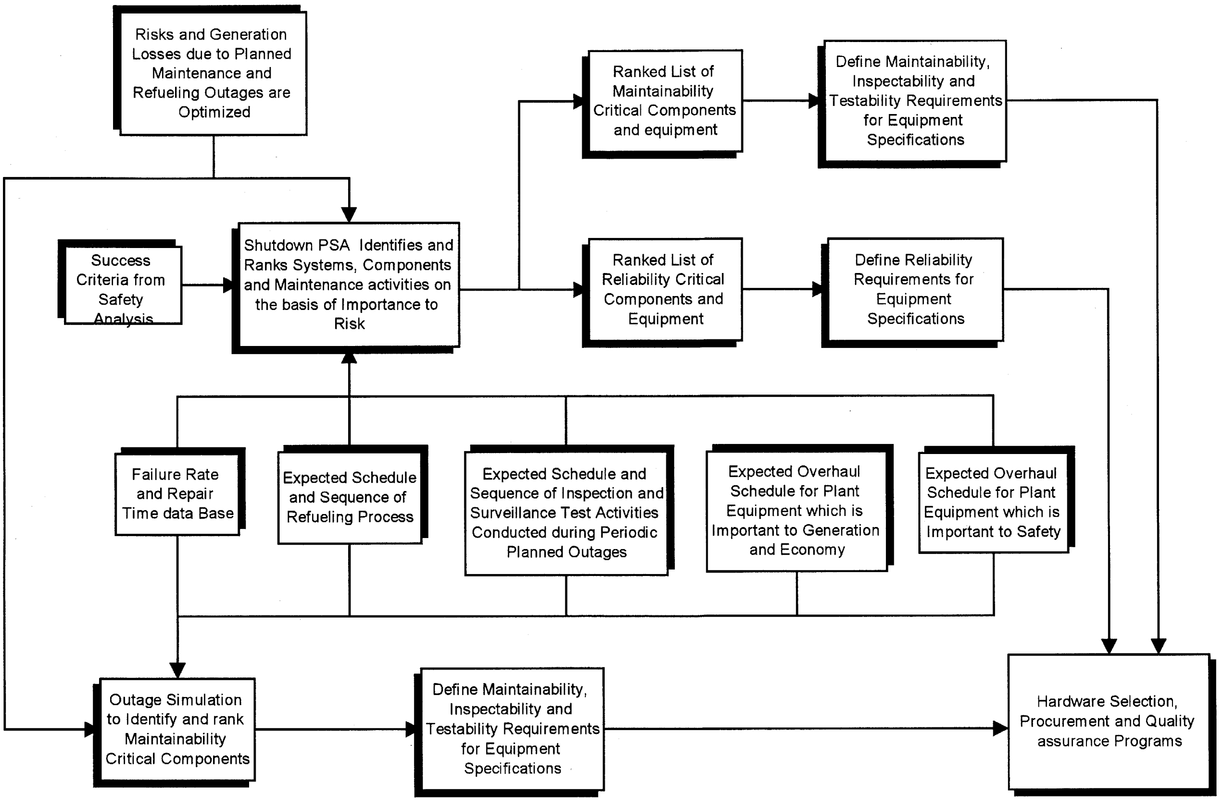

Risks and Generation Losses due to Planned Maintenance and Refueling Outages are Optimized
Ranked List of Maintainability Critical Components and equipment
Define Maintainability, Inspectability and Testability Requirements for Equipment Specifications
Success Criteria from Safety Analysis
Shutdown PSA Identifies and Ranks Systems, Components and Maintenance activities on the basis of Importance to Risk
Ranked List of Reliability Critical Components and Equipment
Define Reliability Requirements for Equipment Specifications
Failure Rate and Repair Time data Base
Expected Schedule and Sequence of Refueling Process
Expected Schedule and Sequence of Inspection and Surveillance Test Activities Conducted during Periodic Planned Outages
Expected Overhaul Schedule for Plant Equipment which is Important to Generation and Economy
Expected Overhaul Schedule for Plant Equipment which is Important to Safety
Outage Simulation to Identify and rank Maintainability Critical Components
Define Maintainability, Inspectability and Testability Requirements for Equipment Specifications
Hardware Selection, Procurement and Quality assurance Programs

*FIG. 3-8. D-RAP – planned optimization.*

The overall process for identifying the list of components which are important to the minimization or optimization of planned outage time relies upon the availability of the important sources of information listed below:

- A compilation of maintenance, overhaul and test activities which are required or recommended by regulatory agencies, vendors and original equipment manufacturers. Later, insights from predictive or reliability centered maintenance analyses will be used to modify these "hard" requirements to produce an optimal set of plant specific requirements;
- A plant database which collates information about failure rates, restoration times and times required to overhaul and test individual equipments;
- The importance of individual shutdown configurations and components which have been identified from the results of the shutdown PSA. These same results can also highlight those particular activities which are particularly risk-important by indicating where human errors can result in initiating events;
- The maintenance and refueling equipment requirements and preliminary outage schedule which will ultimately define the components which are expected to be on critical path.

In the design phase, the information and insights gained about the importance of maintainability, testability and reliability of individual components during plant shutdown will be used to guide the specification, selection and procurement process. The maintainability of these components will be of primary importance and may require some form of simulation to confirm that the plant state allows the maintenance activity to proceed when planned and that the equipment is constructed and installed in a way which provides adequate access, laydown area and minimum interference and provides an environment (heat, noise, light and radiation) which does not severely impact the productivity of individual maintainers.

After identification of the relative importance of individual components, this assessment will probably use a "checklist" approach during design to prevent inadvertent problems from intruding. As construction proceeds, and final equipment selection has occurred, a more detailed simulation may be possible to confirm that the requirements imposed during the procurement process are maintained during construction.

# 4. RELIABILITY ASSURANCE IN OPERATING PLANTS (O-RAP)

## 4.1. INTRODUCTION

In an operating plant, collection of failure, repair and performance data slowly begins to provide a picture of the “plant specific character” of hardware and human performance. In the electrical generation processes, data quickly becomes available to show where problems lie, together with an expression of their failure effects. The importance of failures and their root causes can be derived from analyses of operational and maintenance experience and corrections or changes made to prevent their re-occurrence. In this way the plant maintains the process of “continuous improvement” which is inherent to all availability improvement programmes.

The functional elements of the O-RAP are similar to those used in D-RAP, except instead of having to place full reliance on the inference or synthesis of needed information from a miscellany of analytical and actuarial sources, plant experience becomes the predominant source of information.

In its early years, the amount of plant operational feedback may be limited, but, as the plant matures the amount of information from which to judge the quality of its performance will increase. It is this information which enhances the plant manager’s ability to identify areas of degraded performance, typically evidenced as capability losses, safety system unavailabilities and unreliabilities, initiating event frequencies, plant trips and loss of generation from planned outages.

Management systems used to control nuclear plant operating strategies are analogs to the hardware systems which control the operation of the hardware maintaining generation and core protection functions. There are specific operational objectives (safety, reliability and economy), programmes and activities which are implemented to meet these objectives and a monitoring system which identifies deviations between the desired and actual performance levels. Whenever the deviations between the “goal” levels and observed plant performance exceed their allowable limits, corrective or remedial actions are implemented until a balance is restored.

## 4.2. RAP PERFORMANCE INDICATORS

The idea that the plant can use similar “control” system concepts, e.g. goal setting, performance measurement and comparison, strategic planning and implementation in the form of a continuous loop with negative feedback, is important to an understanding of the role that RAP can play during plant operation (see Fig. 4-1). This same process stimulates maintenance efficiency and safety culture by promoting improved communication and facilitating the integration of different disciplines and organizational entities throughout the plant.

The RAP management control system can conceptually use any defined parameters as control variables, however, as a more practical manner, since the costs of implementation of change are usually measured in economic terms, performance indicators associated with plant capacity factor, safety and risk should generally be converted to their economic equivalent. In this way, all decisions can be made on a consistent basis. Once again, it is important to recognize that the decision maker can select any consistently defined parameter which is convenient and appropriate in maintaining balance or control within each plant performance management system.

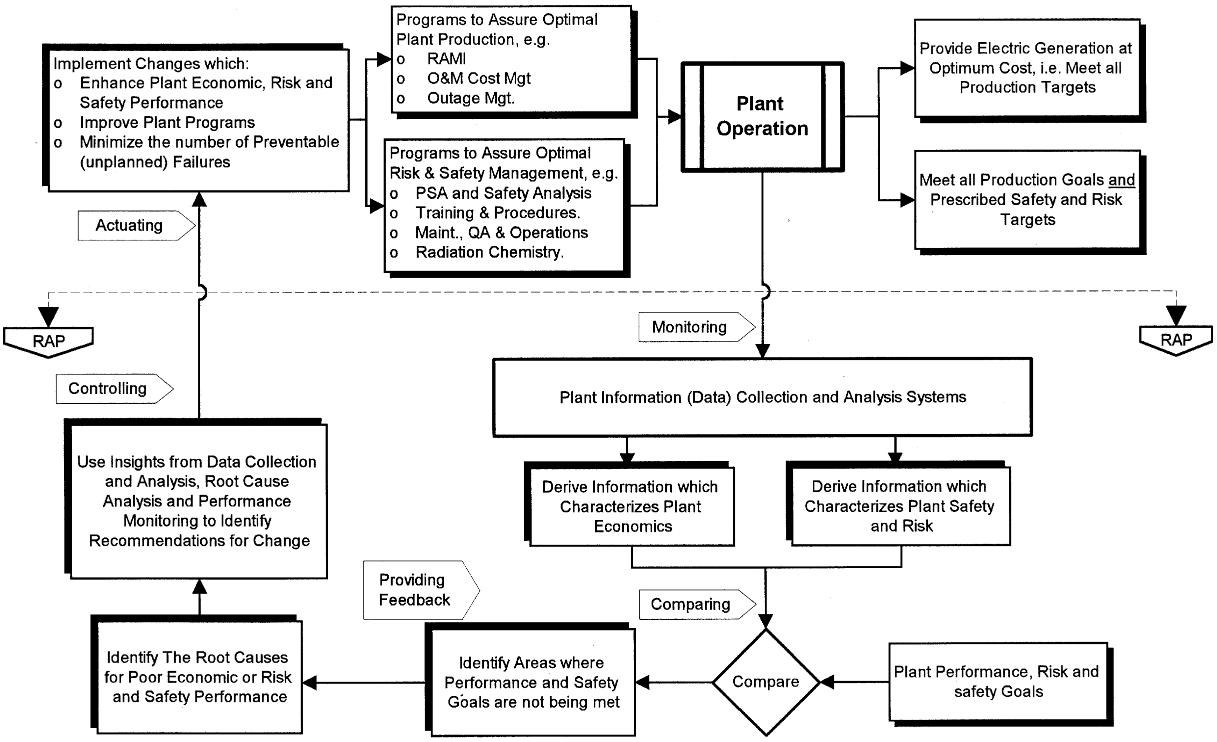

Programs to Assure Optimal Plant Production, e.g.
o RAMI
o O&M Cost Mgt
o Outage Mgt.
Implement Changes which:
o Enhance Plant Economic, Risk and Safety Performance
o Improve Plant Programs
o Minimize the number of Preventable (unplanned) Failures
Plant Operation
Provide Electric Generation at Optimum Cost, i.e. Meet all Production Targets
Programs to Assure Optimal Risk & Safety Management, e.g.
o PSA and Safety Analysis
o Training & Procedures.
o Maint., QA & Operations
o Radiation Chemistry.
Meet all Production Goals and Prescribed Safety and Risk Targets
Actuating
RAP
Monitoring
RAP
Controlling
Plant Information (Data) Collection and Analysis Systems
Use Insights from Data Collection and Analysis, Root Cause Analysis and Performance Monitoring to Identify Recommendations for Change
Derive Information which Characterizes Plant Economics
Derive Information which Characterizes Plant Safety and Risk
Providing Feedback
Comparing
Identify The Root Causes for Poor Economic or Risk and Safety Performance
Identify Areas where Performance and Safety Goals are not being met
Compare
Plant Performance, Risk and safety Goals

*FIG. 4-1. RAP and plant operation (as a control loop).*

The premise for seeking a balance between safety, reliability and economy is outlined in Section 1, namely that increases in safety and reliability "at all costs" is not consistent with the best use of nuclear power as a viable source of central electricity generation and may result in severe mis-allocation of funds which may otherwise be available for risk reduction and safety enhancement in other, more important areas. Each member state will use its own "utility function" to adjust the economic equivalent of safety and reliability to reflect differences in "values" which come from cultural and societal differences and needs.

These values may vary from state to state because of differences in the strategic value of nuclear energy and whether member state has other energy generation options which it can exercise to meet its own particular needs, societal tolerance for nuclear power, in particular nuclear accidents, or whether the value of nuclear energy and any associated costs of failure are determined from the open market place.

The effectiveness of the processes which measure each aspect of plant performance are at the core of the operational RA programme. This information collection and analysis system determines how well deviations from established goals can be identified and how well their causes can be sufficiently well understood to allow the implementation of effective remedial or corrective measures.

### 4.2.1. Economic performance

The indicators for plant economic performance are probably the least complex and most easily defined of all indicators because the linkage between the effects of unreliability of individual contributors and any resultant generation losses is well established and highly visible. Actuarial data collected over a relatively short period of operation will quickly begin to provide the necessary feedback for a management control system, i.e. ensure that the plant is meeting all of its economic objectives, determine that changes are needed, and if so where and what should be changed.

There will be a relatively small, but, important sub-set of potential failures which are not so well identified during the early years of operation, and indeed may not be visible until after a major loss. These are the relatively rare catastrophic failures (primarily major turbine or generator failures) which happen about every ten to twenty operating years but, have the potential for a long term loss of all, or a significantly large part, of the plant’s generating capability. Since the plant rarely experiences an event of this type, its performance must be inferred from “pre-cursor” events or events which occur in other facilities which use similar equipment and indicate or forewarn of design defects or vulnerabilities.

These events are particularly important to “goal setting” because their life cycle contribution is probably included as an average annual unavailability. This means that for many years the goals will be achieved with ease (if there are no catastrophes) and completely missed in the years when there is a failure. Suggestions for resolution of this dilemma are provided in Section 5.1.1.

The performance indicators which have been defined by UNIPEDE, WANO, INPO are examples of the types of performance indicators which may be appropriate for advanced reactors.

### 4.2.2. Safety performance

Feedback about the safety of the plant, i.e. the instantaneous, or average (integrated) core damage frequency, conditional containment failure probability, or risk, is less overt and can usually only be inferred from precursor events or the unreliabilities or unavailabilities exhibited by components in the core and plant protection success paths. This is because severe accidents are so rare that there is never enough actuarial data to provide definitive information of accident frequencies and the relative importance of accident scenarios. Inference or indication of safety performance must be found from solution of the PSA or reliability models which have been adapted to process operational information, often collected at the component or subsystem level.

This information can be processed in several ways, each designed to meet a different aspect of the risk management process:

- Directly incorporate combinations of operational failure events into the PSA and requantify it to estimate the “conditional” risk. This not only determines whether the event is an accident precursor, but also predicts its importance,
- Modify the original component and human failure database to reflect the contributions from the numbers and durations of recorded operational failures and requantify the PSA to estimate the current value of average core damage frequency or other related risk measure,
- Remove the probabilistic contributions to component unavailability from test and maintenance activities which are in the plant PSA, and update the model structure to reflect “real time” plant configuration, i.e. which components/sub-systems are in, and out, of service at any instant of time. Repetitively requantify the PSA to provide an estimate of the instantaneous risk, or the conditional core damage frequency (risk surrogate) for the plant specific configuration,

- Use the insights from the PSA (ranked list of SSCs, human actions, accident scenarios, etc.), to provide a risk based focus for other plant programmes which maximizes the probability of success in preventing and managing accidents so that both their frequency and consequences are minimized.

  Examples include:

  (i) Reliability centered maintenance and maintenance management,
  (ii) Emergency operating procedures and severe accident management,
  (iii) Shutdown schedule optimization and risk management.

Three PSA model types can be used to support the O-RAP, each one of which will be developed to encompass the plant states of interest. These will include consideration of full power, hot and cold shutdown and mid-loop operation, and external threats to the plant (external initiating events) which are appropriate to the application:

- One of these PSAs will provide a baseline assessment, i.e. will represent an updated version of the design PSA and describe the baseline risk profile detailed to the component level,
- The second model will be specially designed for rapid quantification, exclude the average contributions to unavailability from test and maintenance and be amenable to change in “real time” to match actual plant configuration,
- A third set of models may represent a “streamlined” version of the PSA which implicitly carries the detail of the baseline model, modified to allow rapid requantification.

This last particular model is useful when needed to provide support to the plant decision making because its response time is short and it typically provides insights at a relatively high (sub-system) functional level so that the results are consistent with an operational viewpoint. If the tools are available, this model can also be constructed in success space so that it better matches the operator’s view of the plant, which is in terms of success paths, i.e. “what must work to make electricity and keep the core and containment safe”, rather than the PSA analyst’s view point which is more towards the identification of every combination of failures which can result in core damage. Both viewpoints are equivalent, but, the application may better suit one, or the other. This model must produce the same results and insights as the baseline PSA.

Quantification of the baseline and “fast solver” PSA models will provide predictions of the average expected annual core damage frequency and all associated conditional events and probabilities, whereas quantification of the “real time” model will provide instantaneous values of risk (CDF, CCFP, or risk). The integrated average of the instantaneous risk curve should converge with the results from the baseline and fast solver PSAs if the quantification information for each is consistent. There will, however be year to year variations which result from the number of plant modifications which have been implemented.

This description of operational reliability assurance programmes (O-RAP) makes no claim to define these levels, but, merely recognizes their existence and uses them as undefined constraints with which the overall optimization of operational performance can proceed.

### 4.2.3. Importance of feedback experience in the definition and measurement of indicators

The important elements of the O-RAP are analogous to the elements which are part of the D-RA process, and differ only because the O-RAP draws information, primarily, from plant operational experience and the D-RAP uses information from all available sources to characterize the expected plant performance and to predict how well it will work. To be effective the O-RAP must be able to:

- Monitor and identify the operational feedback which is needed to describe levels of plant performance,
- Organize the collection of operational data so that it provides the necessary feedback about human and technical failures,
- Maintain an adequate level of quality assurance in each part of the operational data collection process,
- Assure that there is adequate training provided to all personnel engaged in the collection and processing of operational data,
- Guide the analysis of the data to identify areas in which the plant is operating below their expected levels and determine the reasons for these undesired anomalies,
- Follow through and assure that changes, proposed to enhance plant performance and safety, are implemented.

## 4.3. RELIABILITY, AVAILABILITY, MAINTAINABILITY IMPROVEMENT (RAMI)

Because there are differences in the methods and techniques needed to support these programmes in the areas of safety, reliability and economy, the programme will tend to operate within three different areas. Optimization of “operating economy” will focus on individual areas described by the load duration curve and “operating safety” will embrace an overall scope which is comparable to that encompassed by the PSA. This means that for:

**Generation and economy** — the tools and methods must focus on “reliability, availability and maintainability improvement” and minimizing lost generation from forced outages, forced reductions and planned outages.

**Safety** — the tools must focus on the management of the risks presented by a nuclear facility by ensuring that the CDF, CCFP and individual risk is maintained at an acceptably low level.

The essential ingredients of an operating plant RAMI programme for generation and economy include:

- A clearly defined and consistent approach which provides unique identification for each plant component for which data or information is to be collected and defined requirements for the collection of data which are consistent, complete and unambiguous and adequate to support the needs of the O-RAP;
- A consistent way to identify and classify the root causes and effects of component and human failures so that the resulting information can be analyzed to return the maximum feedback about the effectiveness of plant programmes and management systems;

- A set of "performance indicators" which provide trending and diagnostic information about the performance of individual plant programs which influence the high level generation goals;
- A set of prescribed system or plant level performance criteria which provide a benchmark as economic conditions and the comparative efficiency of the plant changes throughout its life against which the acceptability of plant performance can be measured.

  Note:

  These may change as economic conditions and the comparative efficiency of the plant changes throughout its life;
- A consistent way to rank observed human and hardware failures so that they can be used to direct the efforts of an availability or reliability improvement process, and to allow their comparison with a target which can provide an indication of the potential for improvement, i.e. not only identify the greatest contributors to plant unavailability or unreliability, but, combine this information with an assessment of their potential "improvability" to both justify and prioritize the search for cost effective plant enhancements;
- Practical and consistent methods for assessing the maintainability of individual components and understanding how changes to the plant environment or the physical location and accessibility of the component can influence its maintainability;
- Methods and models which can be used to predict the effects of changes to the plant or the ways it is operated or maintained;
- An economic model which provides a consistent way to directly calculate and compare the worth of incremental changes in plant reliability, availability and maintainability with their estimated implementation cost.

The essential ingredients, elements and objectives for an operating plant RAMI programme to manage risks are:

(a) Maintain average plant baseline risk levels below the established "acceptability" probabilistic criteria, throughout its life. These criteria may be set by the regulatory authority to reflect societal standards, or by the owner, who may select more restrictive criteria to better serve his own specific concerns, or to accommodate increased levels of uncertainty in his risk predictions;

(b) Maintain average plant baseline risk levels below the established "acceptability" probabilistic criteria, throughout its life by using a time dependent failure event database and the PSA results and insights to manage the plant ageing process;

(c ) Not only confirm that the plant has no important "vulnerabilities" and that its risk profile is not dominated by a very small sub-set of contributors, but, also confirm that changes made to the plant during its operational life do not introduce new vulnerabilities.

PSA and RAM (reliability) studies can also be used to confirm that any specific change to the plant will not increase either the frequency or severity of an accident. In the USA these requirements are defined by 10CFR50 Par. 59;

(d) Maintain "instantaneous risk" at an acceptable level as operational demands initiate changes in plant configuration;

(e) Use the results, insights and models from the risk assessment to determine the risk importance of operational events to be certain that:

  - All accident "pre-cursors" are clearly recognized,
  - Remedial actions are taken to prevent their re-occurrence, to a degree which is commensurate with their severity;

(f) Focus the expenditure of resources to improve plant safety in areas which are most important and provide the greatest benefits or return on investment, i.e. use the PSA to:
  - Measure the safety significance of any identified deviations from the plant licensing basis and prioritize remediation activities, whenever they are discretionary, i.e. allowed by the regulatory agency,
  - Establish the worth of all proposed changes to the plant to justify and prioritize their implementation;

(g) Use the results, insights and models from the risk assessment to support all other plant programs by providing a focus for areas in which change is merited, for example, ensuring that:
  - Risk-important human actions are proceduralized and that the operators are well versed in their content and practice them regularly on the plant simulator,
  - Emergency drills are derived from important accident sequences;

(g) Use the results and insights from the PSA to guide the development and implementation of a graded quality assurance programme, in which the quality requirements are commensurate with the risk-importance of the hardware or associated administrative or procedural controls.

Many of these specific applications will be discussed in detail in Section 6. To serve these programmes, the plant must develop a comprehensive PSA with the necessary breadth, depth, fidelity, quality and responsiveness. A brief description of the analytical requirements for the risk assessment process is also provided in Section 6, but, below there is a brief description of the overall performance specifications which should be considered for the PSA when its is used for each of the applications described above.

A flow chart showing how the elements of a typical RAMI programme interact, is shown in Figure 4-2. This does not show how RAMI is used to minimize planned outage losses, only losses caused by forced and maintenance outages.

Though the tools needed to support a RAMI programme are detailed in Section 5 of this report, a brief overview of its more important aspects are provided below.

### 4.3.1. The plant information collection system

To enhance plant performance it is essential that the plant information system provide the necessary feedback to define:

- How well the plant is operating when compared to established goals,
- Where the deviations are occurring,
- Why they are occurring and,
- How to define cost effective solutions to achieve the necessary improvement.

#### *4.3.1.1. Unique identification numbering system*

Having the ability to correctly attributed information collected for individual hardware items so that it can be used to guide the performance management process, means that having a system which unambiguously identifies each plant component and piece part is one of several critical elements of a plant information system.

Ideally, this identification system will follow a national standard so that not only can the plant collect information for each hardware element and report it to a national data repository without having to perform a “translation” into an equivalent nomenclature, but also archive it so that it can be compared to the observed performance of similar components, installed in other plants. If a national or utility standard is not already defined and in use, IEEE Standard 805 (or its equivalent in member states other than the USA) can serve as an important foundation.

An important issue in providing early system definition relates to one of “system boundaries”. The AE, NSSS and other vendors may define system boundaries which reflect their scope of supply, whereas in operation, the system boundaries are usually functional. Achieving a standard from the outset prevents the need for changes later which can be costly if test, maintenance and operating procedures must be changed to correspond.

#### *4.3.1.2. User informational needs*

A matrix of needs should be constructed before the plant information collection system is implemented. Because there are relatively few sources of “raw” data which are available to provide the needed plant performance feedback, it is important to define the complete set from the outset. If this is not done, increased sequential processing of the data to provide the necessary decision-making parameters will result in its heritage and pedigree becoming less well defined and there will be an associated increase in the uncertainty in the analytical products derived from this information. When the raw data collection needs are derived from the user’s perspective and reflect specific needs, the quality of the information remains at its highest level.

### 4.3.2. RAM models

A set of equivalent availability, reliability and maintainability models are developed to provide the relationships between the reliability and availability of individual components and the expected plant capacity factor during the design process. These models take on many different forms, but, the most commonly encountered ones include:

(i) Reliability or availability block diagrams (RBDs or ABDs),
(ii) Fault trees or success trees (FTs or STs),
(iii) Event trees (ETs),
(iv) Monte Carlo simulations to estimate uncertainty.

Generally these methods are embedded in software packages which provide specially defined user interfaces and translate reliability information into a form which can be used directly by the decision maker. As the plant matures, the use of these types of “predictive” models declines and is replaced with models which extract decision-making information from actuarial data:

- Trending and analysis models which operate on actuarial data collected and characterized by operational plant information systems which are used to identify sources of poor performance;
- Root cause analyses which identify the reasons for failures in order to define a technically sound basis for recommendations which prevent their reoccurrence.

### *4.3.2.1. The reliability "SCRAM" model*

The reliability model can be developed successfully with a fault tree in which the "top event" or outcome of interest is defined as "immediate plant shutdown". By structuring the model to mimic the functionality of the reactor protective system the frequency for plant SCRAMs can be synthesized from the unreliabilities of each of the individual components whose unreliability leads directly to plant unreliability.

As always with models that include both event frequencies (initiating events) and event probabilities (subsequential or consequential failures), the naming of events must be very precise to ensure that individual conditionalities are protected and maintained throughout their analysis.

In operation, the results from this model can be used to identify potential sources of SCRAMs so that the plant's SCRAM reduction program can focus on their prevention, as an important first step.

### *4.3.2.2. The reliability "forced outage" model*

The results from the solution of the SCRAM model, typically presented as a set of SCRAM scenarios and their associated frequencies, are used to identify the most important sources of Reactor SCRAMs and their contributing causes. A prediction of the expected down time for each scenario is made for each SCRAM scenario and in combination with the scenario frequency, used to predict unavailability due to full forced outages and their corresponding generation losses.

In operation, these predicted values can be used as targets or preliminary goals for initial bench marking of the overall plant reliability improvement programme. In addition, because the analytical results from the plant reliability analysis identify the important contributors to forced outages, in rank order, they can also focus plant programmes which are implemented to reduce SCRAM frequency or plant down times. This same information can also be used in conjunction with operating experience to guide a SCRAM reduction programme

Though many existing plants rely on an a formal SCRAM reduction programme to maintain plant SCRAM frequency at an acceptable level, whenever a plant make the decision to institute a formal and comprehensive reliability assurance programme, SCRAM reduction becomes an integral part of O-RAP. This specific activity is folded into the plant wide RAMI plan so that all of the reliability engineering methods, techniques and expertise introduced by O-RAP can be exploited in a rigorous manner to maximize the probability of programmatic success. One of the most important tools will involve the development of effective root cause investigation techniques associated with the swift identification of the causes for SCRAM, perhaps guided by an overall SCRAM reliability model, which will attempt to ensure that the plant never has two SCRAMs for the same reason.

### *4.3.2.3. The equivalent availability model*

Repetitive solution of an availability block diagram model in which the success criteria are varied to correspond to the minimum requirements for each selected power level, provide estimates of the probability that the plant capability will exceed this nominal value. Plotting and integrating the resultant probabilities will provide both the equivalent availability and the expected generation losses to forced reductions.

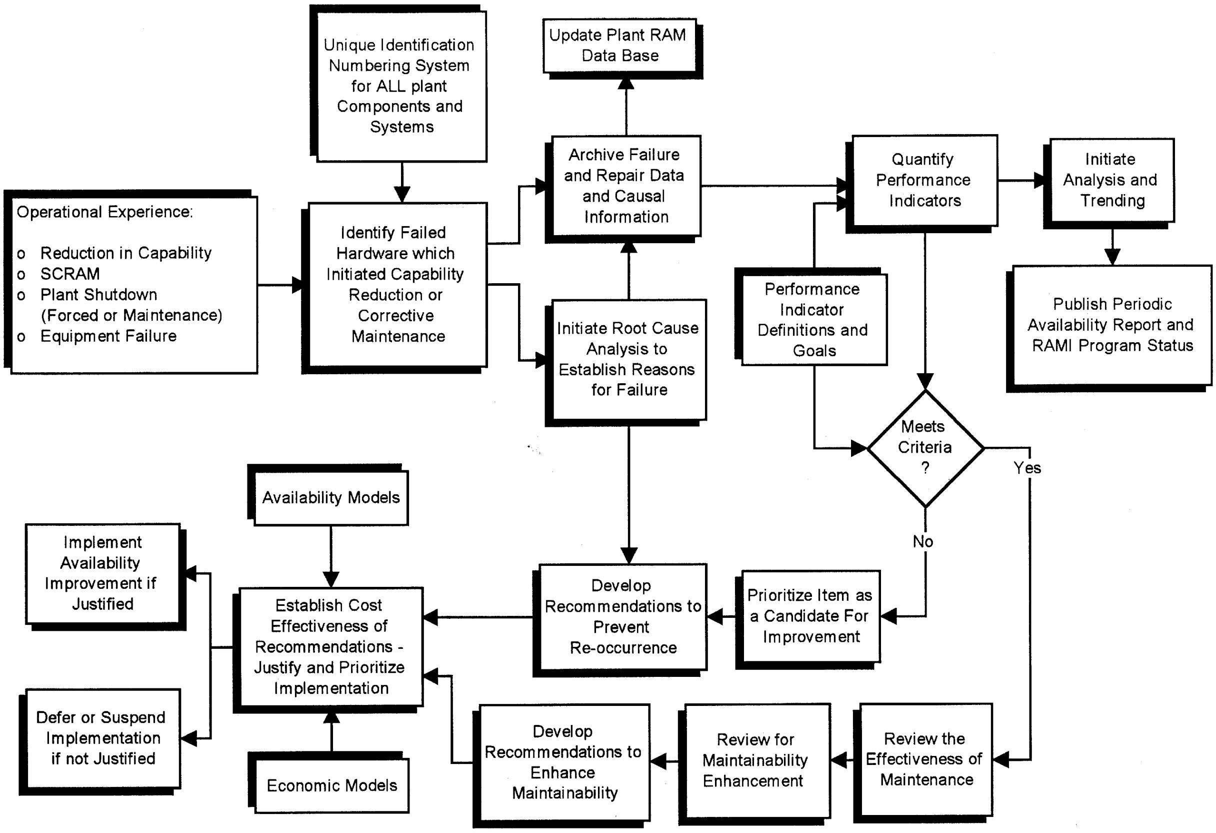

Unique Identification Numbering System for ALL plant Components and Systems
Update Plant RAM Data Base
Archive Failure and Repair Data and Causal Information
Quantify Performance Indicators
Initiate Analysis and Trending
Operational Experience:
o Reduction in Capability
o SCRAM
o Plant Shutdown (Forced or Maintenance)
o Equipment Failure
Identify Failed Hardware which Initiated Capability Reduction or Corrective Maintenance
Initiate Root Cause Analysis to Establish Reasons for Failure
Performance Indicator Definitions and Goals
Publish Periodic Availability Report and RAMI Program Status
Meets Criteria ?
Yes
No
Availability Models
Implement Availability Improvement if Justified
Establish Cost Effectiveness of Recommendations - Justify and Prioritize Implementation
Develop Recommendations to Prevent Re-occurrence
Prioritize Item as a Candidate For Improvement
Defer or Suspend Implementation if not Justified
Economic Models
Develop Recommendations to Enhance Maintainability
Review for Maintainability Enhancement
Review the Effectiveness of Maintenance

*FIG. 4-2. RAMI programme.*

### 4.3.3. The root cause investigation programme

The root cause programme (discussed in detail in Section 6) is a different type of analytical tool but essential to plant improvement because effective root cause and a programme whichfollows through on the implementation of recommendations from the root cause analysis, can prevent re-occurrences. Analytical RAM models augment the insights provided by plant operating data to identify those areas where it is important to attempt to "prevent" or preempt failures which result in SCRAMs, whereas (successful) root cause analysis identifies the causes for a specific SCRAM and identifies a strategy which, when implemented, will prevent it from ever happening again.

Successful root cause analysis will always identify the "management system" failures which enabled or caused the hardware failure. For example, the results from the root cause analysis should answer the questions:

- Why plant maintenance, testing and inspection programs were ineffective in preventing an unplanned failure, or,
- Why plant maintenance, testing and inspection programs failed to detect a degraded condition in an important SSC so that intervention could take place before the unplanned SSC failure occurred.

Unless the underlying inadequacies, weaknesses and vulnerabilities in management systems are identified and corrected, repetitive failures will continue to occur.

A very powerful **goal for a SCRAM reduction programme** is one in which avers a determined effort to **NEVER have two SCRAMs for the same reason**, particularly when the root cause is described in terms of the management system failures which allowed it to happen.

### 4.3.4. Reliability centered maintenance

Reliability centered maintenance represents a powerful programmatic tool which can be used to minimize the number of unplanned failures which lead to SCRAMs or capability reductions. The analytical RAMI models are used to identify the ranked list of "Utility Critical" components in which the importance is a function of both the likelihood of failure and the effects from the failure. The reliability centered maintenance programme uses analytical techniques to examine the failure characteristics of each of these components:

- Performance of a functional failure analyses to identify their important functional failure modes (based on frequency and expected repair time),
- Identification of potential hardware damage states and any associated information which could be available for detection and diagnostic systems to monitor the progression of individual failure modes,
- Analysis of plant diagnostic and monitoring systems to determine whether the failure mode/damage state information is detectable and whether it is possible to establish a progression threshold which ensures that unplanned failure will not occur between planned maintenance overhauls or refurbishment activities,
- Identification of maintenance actions which are effective in preventing the initiation and progression of flaws which result in functional failures,
- Prediction of how long the hardware is expected to operate without failure in the absence of any preventive maintenance strategies,
- Selection of a condition directed or time directed task which will prevent unplanned failures of the "utility critical" components from the identified important functional failure modes.

### 4.3.5. Plant risk management

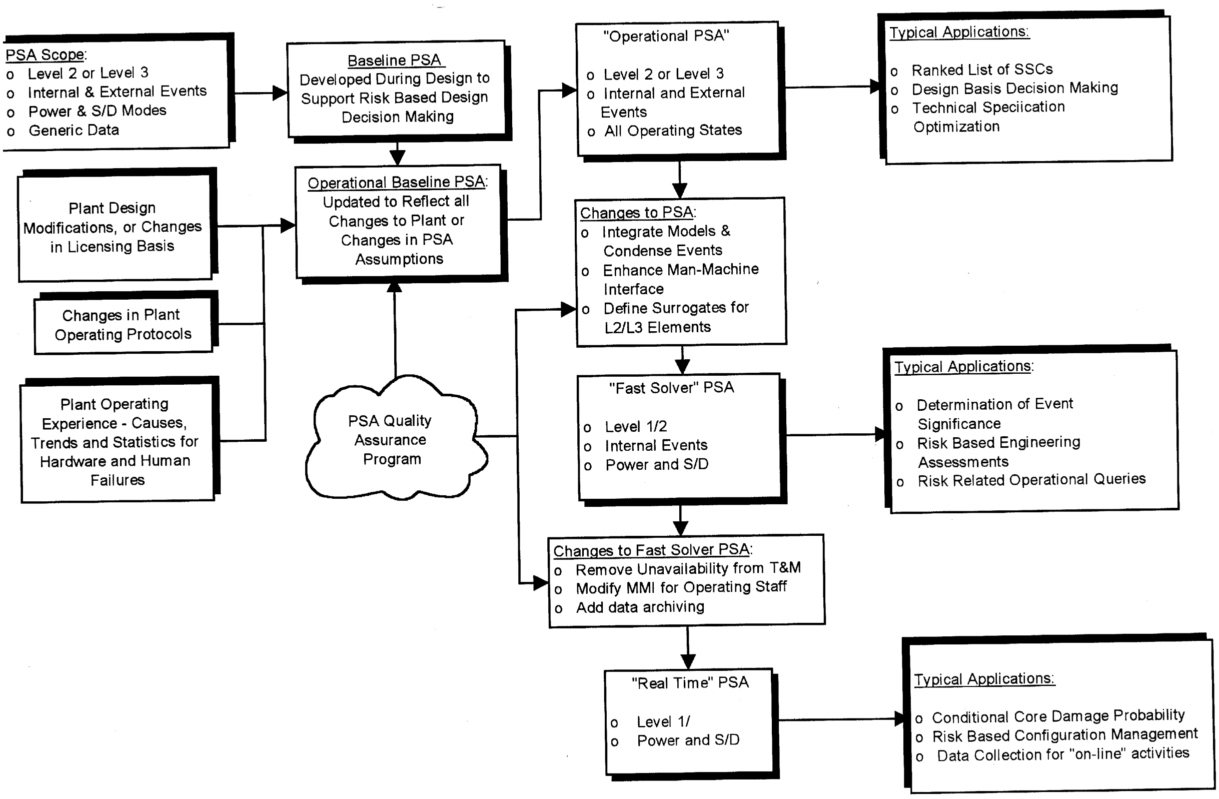
A typical operating plant risk management programme focuses on many issues, but, in each case there is a need for an analytical tool or "risk or safety assessment" which provides the plant staff with the ways of predicting "importance to safety". The primary reason for having to use a PSA to assess safety significance comes from the fact that accidents are very rare (~1E-5 per reactor year) so there is very little actuarial data for severe accidents which can be used as a basis for comparison when safety system failures occur.

The second important reason is that the plant response to an initiating event can be very complex and the cause and effect relationships which are very visible between hardware failure and plant capability reductions can be obscure when related to loss of core and plant protective functions. An idea of how different types of PSA models may be needed to meet the different needs of a typical plant decision maker are shown in Fig. 4-3. When the PSA is used to support risk management activities it must have a quality level which is commensurate with its application and have adequate documentation to clearly identify the boundary conditions and assumptions which were assumed during its development.

Some of the more important elements and objectives for an overall plant risk management programme are described below, and in many cases, further described in Section 6.

### *4.3.5.1. PSA performance specifications*

An important element of the PSA is that it has adequate scope, fidelity and explicit detail and can provide the needed results within the time constraints imposed by the nature of the decision making process. The actual performance specifications must be derived from the applications, it is only then that the nature of the required tools can be fully discerned. From the above description of the possible applications, it becomes clear that there is a need for suite of PSA models, each of which provides comparable results, albeit somewhat different in detail, character and speed.



PSA Scope:
o Level 2 or Level 3
o Internal & External Events
o Power & S/D Modes
o Generic Data
Baseline PSA
Developed During Design to Support Risk Based Design Decision Making
"Operational PSA"
o Level 2 or Level 3
o Internal and External Events
o All Operating States
Typical Applications:
o Ranked List of SSCs
o Design Basis Decision Making
o Technical Speciication Optimization
Plant Design Modifications, or Changes in Licensing Basis
Operational Baseline PSA:
Updated to Reflect all Changes to Plant or Changes in PSA Assumptions
Changes to PSA:
o Integrate Models & Condense Events
o Enhance Man-Machine Interface
o Define Surrogates for L2/L3 Elements
Changes in Plant Operating Protocols
Plant Operating Experience - Causes, Trends and Statistics for Hardware and Human Failures
PSA Quality Assurance Program
"Fast Solver" PSA
o Level 1/2
o Internal Events
o Power and S/D
Typical Applications:
o Determination of Event Significance
o Risk Based Engineering Assessments
o Risk Related Operational Queries
Changes to Fast Solver PSA:
o Remove Unavailability from T&M
o Modify MMI for Operating Staff
o Add data archiving
"Real Time" PSA
o Level 1/
o Power and S/D
Typical Applications:
o Conditional Core Damage Probability
o Risk Based Configuration Management
o Data Collection for "on-line" activities

*FIG. 4-3. Use of PSA in operational decision making.*

### *4.3.5.2. The baseline PSA*

The baseline PSA will provide a detailed description of the plant risk profile, in terms of:

- Core damage frequency and a ranked list accident scenarios which are important to CDF;
- Importance measures for individual failure events which affect plant core damage frequency;
- A ranked list of systems, structures and components which are important to safety;
- Important containment accident sequences and damage states;

- A ranked list of characterized core damage scenarios that result in a release of fission products;
- A grouped list of source term release categories and associated frequencies whose effects on the surrounding environment can be modeled to predict individual risk and economic impact.

The baseline PSA will be derived from information which represents the finalized plant design, and will maintain current whenever changes to the plant are made in the form of changes to the hardware, software or administrative systems. Ideally, it will be developed to meet all QA programme requirements which are imposed upon a design basis calculation so that it can be used with confidence in assessing the adequacy or merits of changes to the plant design basis. The nature of the plant technical specifications, or other plant administrative controls will determine how the validity of the assumptions within the PSA are to be maintained throughout the operational life of the plant.

The PSA should be performed for each discrete plant state of interest, typically full power, low power, hot and cold shutdown and mid-loop operation and should reflect the effects of both internal initiating events and threats which are external to the plant, e.g. fires, floods, severe weather, earthquakes, volcanism or threats posed by other industrial facilities or activities in the vicinity.

Initially the PSA will be quantified with generic hardware failure rates and repair data which has been screened for applicability to the plant. Later, it will be updated as plant specific failure and repair experience becomes available. This is usually done with Bayesian techniques, although several statistical approaches are possible, provided they operate on an appropriate population.

Human failure data used in the baseline PSA will be derived from an analysis of the expected tasks and the information, the procedural guidance provided to the operator and the assignment of a screening value which is derived from a recognized HRA data source. As procedures change and information about the human role in operating events and simulator experiments becomes more specific, all important human actions and their associated HEPs will be reviewed and updated to confirm that they reflect all plant specific conditionalities.

Because the actual time dependent plant configuration changes cannot be modeled explicitly in the PSA, unavailability contributions from test and maintenance activities average are used to reflect the average number of hours that the plant system may be in a specific configuration during some period of time, or the probability that the system will be unavailable at the time of a demand which occurs randomly over the interval. As the plant matures, first, it is important that the plant not exceed these expected unavailabilities without first calculating the corresponding effects that it has on risk. Second, if the plant regularly experiences system unavailabilities which differ from those in the baseline PSA, the baseline PSA data will be updated and the risk requantified.

The solution time for this model is of lesser importance than that of the other plant models to be discussed because, primarily it is intended to serve as a reference for each of the other PSA decision making models, and will not be routinely re-solved. However, if possible the integrated suite of level 1, 2 and 3 plant models should be structured in “modular” form, or with an equivalent convenient structure, to facilitate determination of the effects from a change with only a partial re-solution. This also means that the documentation for the models should also be structured to allow rapid updating, and that it should include extensive indexing so that a search can be quickly and effectively undertaken to determine where an update may be necessary. Having the ability to quickly determine whether the results from the analyses performed for external initiating events or non-full power states modeled in the PSA are affected by any specific change may be important in controlling the scope and minimizing the resources needed to update the PSA.

#### *4.3.5.3. Fast solver PSA*

The fast solver PSA should contain an equivalent amount of information as the baseline, however, the detail may be implicit, e.g. instead of defining each individual component failure event, they are rolled up to the sub-system level and represented as independent super-components, with all associated functional dependencies relocated to the subsystem level. This reduction in detail and model complexity and decreases the required solution time because it moves some of the calculation outside the model. This model may also be fully integrated, i.e. where the baseline model may use fault trees and event trees to represent the plant, the fast solver may combine the functional response and systems models into a streamlined version or ideally, into a single model which manipulates both frequencies and probabilities within a single logical representation of the plant.

The quantification of failure frequencies and probabilities for initiating events and sub-system failures will be synthesized outside the PSA from the individual contributors defined in the baseline PSA. The only real constraint on the streamlining process is that the fidelity of the logic in the baseline PSA model must be preserved, i.e. condensation must be limited to the grouping of component failure modes whose effects can be combined under an “OR” gate, and all common cause failures which cross sub-system boundaries must be maintained.

Whether there is a need to model each power state, each category of external initiating event and whether the Level 2 (containment) and Level 3 (consequences) models should be included will depend upon the specific needs of the plant decision-making process and whether the baseline PSA can meet these needs. f so, the use of a Level 1 internal event fast solver PSA may be adequate, if not, it will require augmentation as necessary.

The time required to modify the models and obtain the necessary insights and results needed to answer the questions raised by the issue of concern will vary, but, it typically should be achievable within an hour or so. This is because operational problems have a relatively short fuse, i.e. after a problem occurs, there is frequently a need to assess its importance very quickly because the importance will often dictate the nature of the required response. The fast solver PSA models will be used most frequently in the assessment of importance for operating events (hardware, human or software failures) or deviations from the plant licensing basis which are discovered during plant operation. It may be necessary to confirm the findings with the baseline PSA at some later time, when there is more time available to complete the activity.

The adaptability of the fast solver, which results from its streamlined construction, places an additional burden on its documentation and fidelity to the baseline PSA. It must be traceable to the design basis if the results are to have credibility, and the models must be very well documented so that when the analyst or decision maker implements changes to mimic actual plant conditions he fully understands any implicit assumptions or model limitations which can affect the results or insights. Because these PSA models will be used by the plant technical support staff, not just the PSA specialists, the man-machine interface must focus on the transfer of information needed to resolve decision making issues and not necessarily include the much more detailed, and complex, risk-sensitive insights and relationships captured within the set of outputs provided by the suite of computer codes which make up a typical PSA software package.

#### *4.3.5.4. Real-time PSA solver*

The third type of PSA tool, the near “real-time” PSA solver is used to manage the plant’s operating configuration. Instead of using a probabilistic estimate of the test and maintenance contributions to component and subsystem unavailability, the streamlined PSA is modified to reflect a plant configuration in which all sub-systems and components are unaffected by test and maintenance activities. As changes to the operational plant configuration are proposed to remove and restore sub-systems and components from service so that test and maintenance activities can be performed “on-line”, corresponding changes are made to the PSA and repetitive resolution used to predict the expected shift in core damage frequency.

Comparison of the magnitude of the shift with a set of prescribed criteria provides the basis for determination of its acceptability. If the proposed change is acceptable, implementation is initiated and the model updated to show the configuration. If the proposed change is unacceptable, implementation is deferred, and the model left in its unmodified state, ready for evaluation of the next proposed change.

Because this PSA will be used by the plant operating staff, it should have an easily used interface which places minimal reliance on knowledge of PSA methods and techniques and exploits the operators knowledge of plant operating protocols and the plant itself. Because the results from the analysis should be available “on demand”, the PSA should have a solution time which is less than 5 minutes.

There are two possibilities for the model solution process, to resolve the PSA or to manipulate the cutsets or results from the PSA. Both provide adequate results provided that the cutsets provide a sufficiently broad database to encompass all expected risk important system configurations, i.e. nothing of potential importance has been truncated from the model. Inadvertent truncation is possible for very reliable components, whose failure probability has little effect on CDF, may be in sequences which are truncated, whereas in real time they may be set a “failed” state, i.e. their probability of failure set equal to “one” when they are removed from service. All components which can be isolated or removed from service for test or maintenance should be addressable within the PSA.

#### *4.3.5.5. Other PSA models for risk management*

The extent to which these active PSA models are needed, instead of relying on the ability of the baseline PSA to provide the basis for a set of sensitivity studies which can provide the necessary guidance will in large measure depend upon the degree of configurational flexibility offered by the plant technical specifications or administrative controls and constraints.

The “risk matrix” method for risk based configuration best demonstrates why the above statement is true. With this approach to risk based configuration management, the conditional core damage frequency for each expected, and allowed, out-of-service sub-system or train combination is pre-calculated with the baseline PSA. The results from these calculations are portrayed in a matrix, so that when the operator wishes to place the plant in a specific configuration, he first checks the matrix, and if the intersect for the combination indicates that it is acceptable, the plant is placed in that configuration. These decisions are typically made to facilitate on-line maintenance.

With the very restrictive technical specifications common to US nuclear plants, the approach is viable, however, as the amount of allowed flexibility increases, the number of combinations increases exponentially, and the practicality of the matrix decreases, unless it is managed within a computer program. The expected future increases in the use of risk based, or risk informed, regulations will offer the opportunity for greater flexibility in the technical specifications. This means that the primary operational constraints may be associated with maintaining the validity of the assumptions made in the plant PSA. In this case, the number of possible combinations may preclude any approach which does not involve the real time re-solution of the PSA.

# 5. DESIGN RELIABILITY ASSURANCE — INDIVIDUAL PROGRAMMES

## 5.1. INTRODUCTION

This section of the guidebook provides a description of each individual RA programmatic activity which will probably be needed in a comprehensive design reliability assurance programme (D-RAP). Activities which have an operational focus are described in Section 6. The programmatic approaches presented in these two sections have been assembled from experience gained by various utilities during the implementation of RAMI and risk based management activities. These approaches will of necessity have to be tailored to meet the specific requirements imposed by the organizational culture and regulatory environment which exists within the nuclear community in each Member State.

## 5.2. DESIGN RELIABILITY ASSURANCE

The design review process for reliability assurance represents the first major programme element in which there may be an impact from the application of D-RAP. This is because the review process must not only follow conventional practice in reviewing and comparing the design to all deterministic criteria and requirements imposed by either the plant owner or cognizant regulatory authorities, but, also compare the predicted performance of the design with its prescribed probabilistic criteria. The design team will then use the results from the RA process to exploit any available opportunities for discretionary change to optimize the design.

The insights from this high level review process are used to focus the attention of the design team onto issues which are important to the reliability and maintainability of SSCs, which in turn have an identified level of importance to plant economic and safe operation. This same rank-ordered list of SSCs which guided the designer, will also serve to guide the review because it identifies both important SSCs and the reasons for their importance. This gives the reviewer the chance to confirm that all available opportunities to learn from the analytical insights and enhance the design have been exploited.

As the design team develops the project schedule and implements detailed project specific control and management procedures which will assure its effective and timely implementation, the complementary procedures used to formalize the D-RAP review process should integrated into the overall set of project management procedures.

## 5.3. GENERAL DESIGN REVIEW

An overview of the multi-step D-RAP design review process is shown in Figs 5-1 and 5-2.

This review process has several broad functional objectives, namely, to confirm that the:

- Plant conforms to the deterministic requirements imposed on the design by regulatory or industry requirements, e.g. general design criteria, industry codes and standards or other commitments;
- Reliability and availability models are of adequate quality and scope;
- Results from the analyses are correct, and correctly interpreted;
- Identification of dependencies, e.g. common cause failures, human factors, internal and external hazards, is complete;
- Plant can meet, or exceed, each pre-defined probabilistic economic and safety criterion;

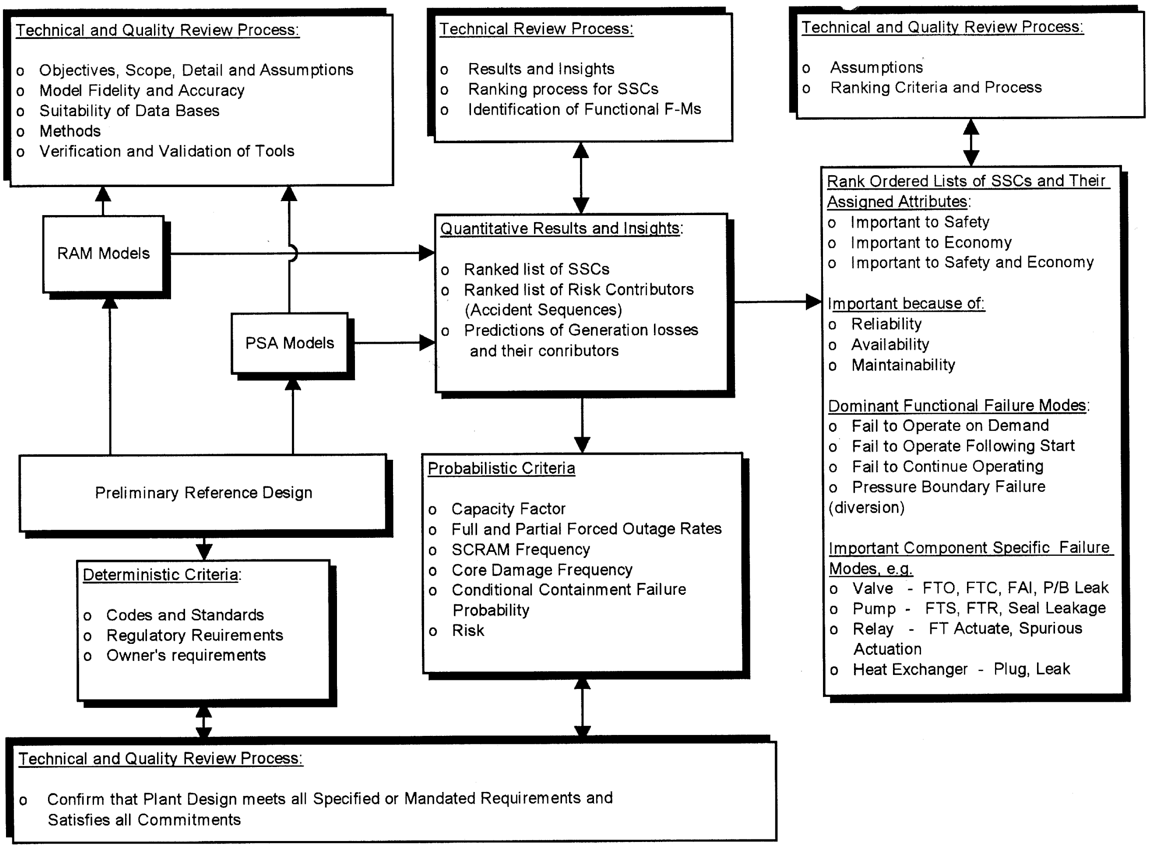

Technical and Quality Review Process:
o Objectives, Scope, Detail and Assumptions
o Model Fidelity and Accuracy
o Suitability of Data Bases
o Methods
o Verification and Validation of Tools
Technical Review Process:
o Results and Insights
o Ranking process for SSCs
o Identification of Functional F-Ms
Technical and Quality Review Process:
o Assumptions
o Ranking Criteria and Process
RAM Models
PSA Models
Quantitative Results and Insights:
o Ranked list of SSCs
o Ranked list of Risk Contributors (Accident Sequences)
o Predictions of Generation losses and their conributors
Rank Ordered Lists of SSCs and Their Assigned Attributes:
o Important to Safety
o Important to Economy
o Important to Safety and Economy
Important because of:
o Reliability
o Availability
o Maintainability
Dominant Functional Failure Modes:
o Fail to Operate on Demand
o Fail to Operate Following Start
o Fail to Continue Operating
o Pressure Boundary Failure (diversion)
Important Component Specific Failure Modes, e.g.
o Valve - FTO, FTC, FAI, P/B Leak
o Pump - FTS, FTR, Seal Leakage
o Relay - FT Actuate, Spurious Actuation
o Heat Exchanger - Plug, Leak
Preliminary Reference Design
Probabilistic Criteria
o Capacity Factor
o Full and Partial Forced Outage Rates
o SCRAM Frequency
o Core Damage Frequency
o Conditional Containment Failure Probability
o Risk
Deterministic Criteria:
o Codes and Standards
o Regulatory Reuirements
o Owner's requirements
Technical and Quality Review Process:
o Confirm that Plant Design meets all Specified or Mandated Requirements and Satisfies all Commitments

*FIG. 5-1. D-RAP design review process (rank-ordered list of SSCs).*

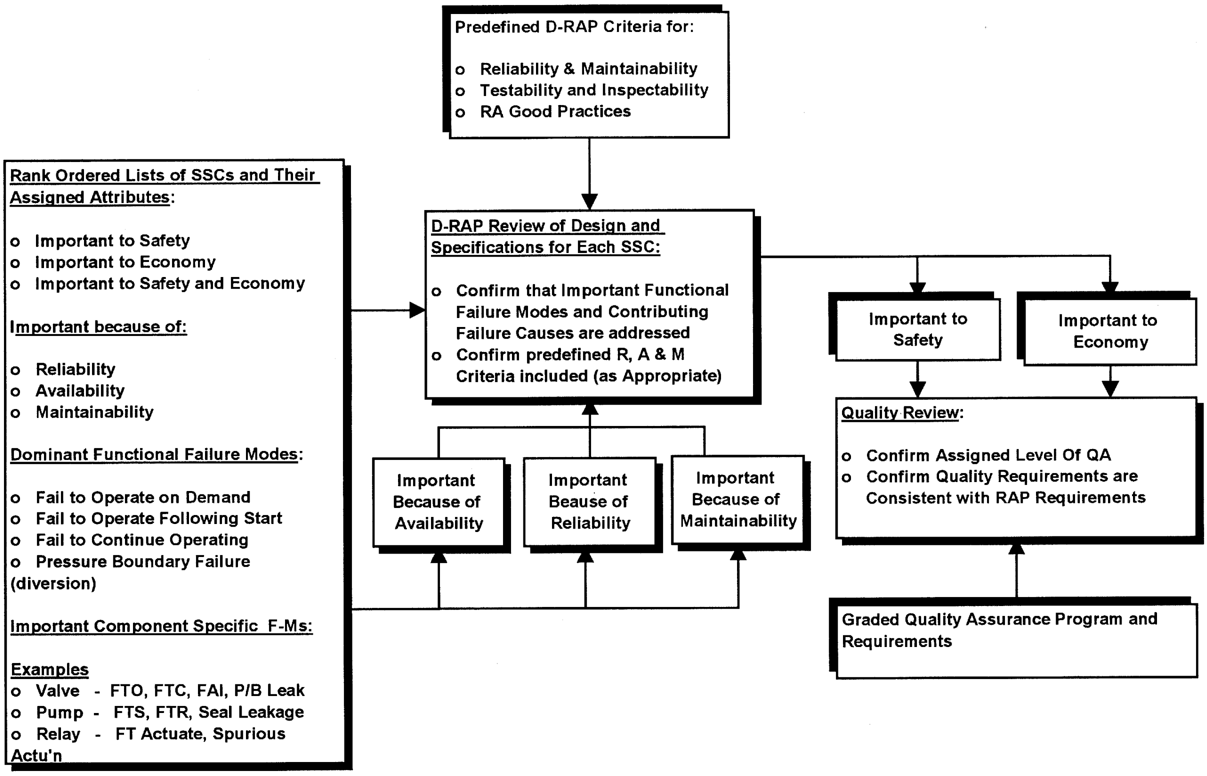

Predefined D-RAP Criteria for:
o Reliability & Maintainability
o Testability and Inspectability
o RA Good Practices
Rank Ordered Lists of SSCs and Their Assigned Attributes:
o Important to Safety
o Important to Economy
o Important to Safety and Economy
Important because of:
o Reliability
o Availability
o Maintainability
Dominant Functional Failure Modes:
o Fail to Operate on Demand
o Fail to Operate Following Start
o Fail to Continue Operating
o Pressure Boundary Failure (diversion)
Important Component Specific F-Ms:
Examples
o Valve - FTO, FTC, FAI, P/B Leak
o Pump - FTS, FTR, Seal Leakage
o Relay - FT Actuate, Spurious Actu'n
D-RAP Review of Design and Specifications for Each SSC:
o Confirm that Important Functional Failure Modes and Contributing Failure Causes are addressed
o Confirm predefined R, A & M Criteria included (as Appropriate)
Important to Safety
Important to Economy
Quality Review:
o Confirm Assigned Level Of QA
o Confirm Quality Requirements are Consistent with RAP Requirements
Important Because of Availability
Important Beause of Reliability
Important Because of Maintainability
Graded Quality Assurance Program and Requirements

*FIG. 5-2. Review of attributes for important SSCs.*

- Rank-ordered list of SSCs is well documented and founded on a technically sound set of assumptions and that the database used to perform the ordering is appropriate to the plant design;
- Attributes assigned to each SSC adequately define the reliability, maintainability, testability and inspectability issues which are of importance to their specification, procurement, manufacture, construction or installation;
- Each reliability critical SSC is correctly and accurately categorized so that any use of this information in the specification of the individual SSC quality assurance requirements to be imposed by the plant graded QA programme, will be entirely appropriate;
- Procurement, installation and construction specifications for each system, structure or component address each relevant reliability, maintainability, testability or inspectability issue of importance to plant reliability, safety or economy;

### 5.3.1. Reference design review

The multi-step review process begins with confirmation that the preliminary reference design meets all of the necessary criteria defined by the Requirements document or the plant owner because they reflect:

- Requirements mandated by regulatory authorities,
- Commitments to meet specific industry codes and standards,
- Agreements to conform to specific industry requirements,
- Specific requirements needed to meet corporate economic objectives.

Early confirmation of the adequacy of the design to meet all deterministic criteria which have been imposed on the design is critical, because any discrepancies discovered later in the design process may require changes that affect the procurement, installation and operation schedule and result in a severe economic impact.

Though not explicitly discussed on the process flow chart shown in Fig. 5-1, this review also provides an opportunity to look at potentially important future requirements which may be imposed, and determine whether the design can accommodate them with limited modifications or changes in the procurement cycle. In case, their incorporation should be considered while the design remains on paper. When the need or desirability for change is identified early in the design, changes can often be made very cost effectively.

### 5.3.2. RAM and PSA model reviews

It is imperative that the review of the RAM and PSA models is initiated early in the design process if they are to be used with confidence during the successful development of the rank-ordered list of SSCs, central to the D-RAP process and of great importance to the design team.

This activity is not actually a review of the plant design, but it provides assurance that each quantitative PSA or RAM model has the requisite quality, fidelity and scope to be used to support definition of the plant design basis.

Though initially the finer details of the design may be poorly defined, the RAM and PSA models must have sufficient "quality assurance" to ensure that they correspond to the "as is" design throughout the design phase, and that they can be changed throughout the life of the plant design and during its operational life without losing “configuration control”. The upgrading and updating process which maintains the correspondence between the RAM and PSA models and the plant design is discussed in Section 2 and shown in Fig. 2-9.

### 5.3.3. Results from PSA and RAM analyses

The results of the RAM and PSA analyses are critical to the D-RAP process because the rank ordered list of SSCs that they produce becomes the guiding force for many RA programmes and RAP activities. This implies a strong need to perform a detailed review of the RAM and PSA results to confirm that there are no computational or modeling mistakes nor errors in assumption which challenge their validity. The reviewer must:

- Compare the overall results with those from similar plants and confirm that the predicted absolute values for each performance parameter are reasonable and that when the causes for these values are examined, they present a consistent picture of the risk profile or capacity factor for the plant,
- Perform a “Limited” independent assessment of the PSA and RAM analyses, for example:
  (i) Use availability block diagram analyses to perform an independent assessment which provides approximate estimates of the expected plant capacity factor and their contributing factors to confirm or question the results from the detailed analysis;
  (ii) Map the results from the PSA onto a plant specific hierarchical functional dependency network which has been derived from design information from the design basis and the PSA to confirm that the PSA results are faithful to the plant. The master plant logic diagram (MPLD) described in Section 5.16 provides an example of a hierarchical network. A mapping of the qualitative PSA results onto the MPLD, or its equivalent, will confirm that:

    (a) Each accident scenario predicted by the level 1/2 PSA results is reasonable;
    (b) The modeled plant functional response to transients and other accident initiating events is consistent with its expected behavior;
    (c) The functional and system models use appropriate success criteria;
    (d) The results reflect the actual plant support system infrastructure;
    (e) All feasible functional success paths which play a role in the mitigation of core damage accident scenarios have been credited;
    (f) Modeling of the relationships between initiating events and the front-line and support system network reflect actual plant design.

This MPLD can be extended to provide additional support for the design review process, beyond concerns raised by level 1 PSA issues:

(i) Extension to include level 2 systems and their dependencies so that the integrated effects of failures can be reviewed to confirm adequate diversity and redundancy,
(ii) Addition of Physical Locators to events in the MPLD to confirm adequate physical separation of functional success paths which may be susceptible to internal fires, floods or external events for indicating dependencies.

The database used to quantify the PSA and RAM models should be reviewed to confirm that it is appropriate for the plant under study and that the failure rates and restoration times are generally consistent with those used in other studies.

### 5.3.4. SSC ranking and SSC attributes

After the PSA and RAM models and the computational methods used in their quantification have been reviewed, the review must be expanded to include the development of the resultant rank ordered list of SSCs and their associated attributes. Most of the information will be derived from the RAM and PSA models in ways similar to those described by the following.

#### *5.3.4.1. Absolute importance of SSC*

Because the importance measure for each SSC will be used to guide the D-RAP process and perhaps dictate the requirements imposed on each SSC during its design, specification, procurement and construction, it is important that the measure is an aggregate of each contributor to its probability of failure.

##### 5.3.4.1.1. Importance to safety

PSAs tend to decompose the SSC into its constituent failure events, e.g. “Out of Service due to test and maintenance”, “failure during stand-by operation”, “failure on demand” and “failure to run following successful start”. If the importance measures for each of these are calculated as independent events, each may have a relatively low calculated value, however, because they are all important to the probability of failure of the SSC programme, an aggregate contribution of each individual failure mode should be used when ranking SSCs for the D-RAP.

##### 5.3.4.1.2. Importance to reliability

The prediction of measures of importance for individual SSCs with the RAM reliability analysis used to predict SCRAM frequency and full forced outage rate raises issues which are similar to those encountered in the PSA. This is caused by the tendency to break down the functional failure modes into their individual contributors so that when they are calculated, they must be re-aggregated to the SSC level.

##### 5.3.4.1.3. Importance to equivalent availability (EA)

The problems associated with the effects of failure mode decomposition on SSC importance becomes less important issue when predicting the availability of normally operating systems. In these analyses, the high level dominant functional failure mode for normally operating components, e.g. loss of flow or loss of cooling, generally provides an adequate description of the failure event so decomposition into detailed failure modes is generally unnecessary.

The difficulty in assigning importance measures to individual SSCs by RAM (equivalent) availability analysis arises with the need to build, quantify and combine the results from several power-state specific models. For these analyses, it seems appropriate to use an “availability importance measure” in which the ratio between a change in SSC availability to the corresponding change in plant equivalent availability become representative of SSC importance.

The difficulty in calculating this importance measure is logistical, merely, because the results from the individual power state models must be combined to produce the EA curve, which in turn must be integrated to calculate the change in EA. This would be done in turn for each of the individual SSCs which comprise the EA model.

### 5.3.5. Measures of importance

**First**, the design review for the SSC ranking process, which is crucial to the ultimate success of D-RAP, will focus on providing assurance that:

- SSC importance is the result of the integration of the predicted importance for each individual failure mode,
- Predicted measures of SSC importances are consistent, i.e. reflect the expected characteristics induced by symmetry within the plant support system and front-line system architecture. Inconsistency in predicted importances, e.g. two functionally similar pumps, “A” and “B”, which have significantly different predictions of importance, may be indicative of inappropriate modeling simplifications.

**Second**, the design review process will focus on the interpretation of the results from the SSC importance Calculations, and confirm that:

- Interpretation of the results from each importance measure prediction is used in an appropriate manner in guiding the categorization of each SSC, i.e.
  (a) the categorization indicates whether reliability, availability or maintainability are important,
  (b) the dominant functional failure mode, and important component specific failure modes are identified and that there is sound technical justification for their selection,
- Overall interpreted measures of safety System importance are consistent with the F-V vs. RAW plot scheme suggested by Section 5.5.4.

This review of SSC ranking process should provide assurance that the master list of rank-ordered SSCs and their associated failure mode categorizations, have sufficient quality and technical justification to guide the design, procurement, manufacture and installation process.

This information will guide the design team by providing it with an indication of:

(i) The reliability and maintainability issues which make each SSC important so that the design can be guided towards minimizing their effect,
(ii) The magnitude of the potential benefits from improvement so that resources can be applied towards enhancement in areas where the payback is likely to be the highest.

### 5.3.6. Comparison with the prescribed performance criteria

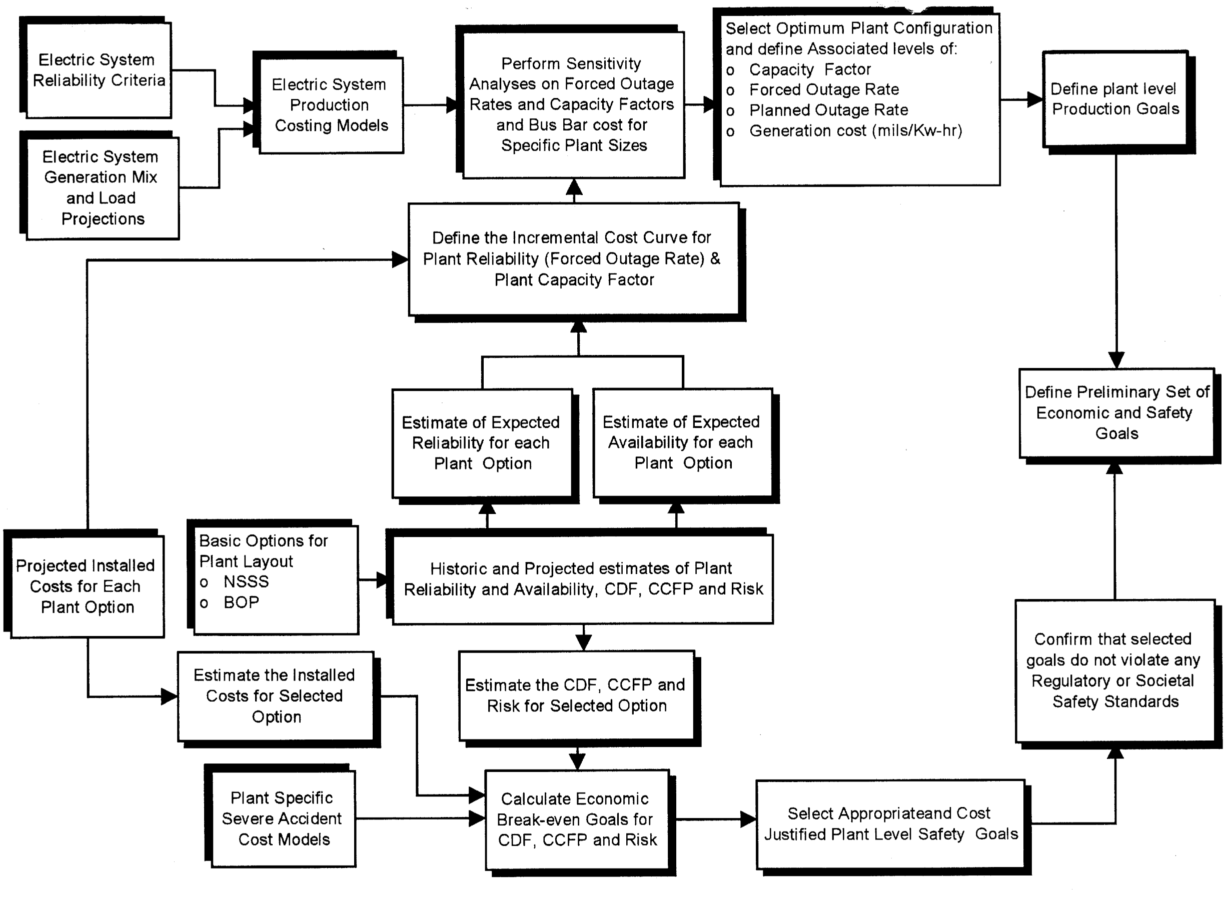
Following confirmation of the quality of the RAM and PSA models and their fidelity to the proposed design, the D-RAP design review process will confirm that the design can be expected to meet each of the prescribed economic and safety performance goals. Insights from the prioritization of SSCs and the absolute values of performance predicted by the models will be used to provide preliminary confirmation.

Where design goals are not satisfied by the preliminary reference design, the information presented by the relative performance indicators for SSCs will be used to identify areas in which design enhancement is able to provide cost-effective changes which lead to satisfaction of the high level goals.

The iterative nature of this task emphasizes the need for effective design configuration control so that as changes are made and detail is added as the design matures, the review process can effectively focus on the changes and not necessarily have to go revert to a re-review of earlier decisions and justifications.

## 5.4. DEVELOPMENT OF PERFORMANCE GOALS FOR SSCs

During the design process, the initial set of SSC performance goals will be derived from actuarial data and expert judgment. These goals will be further refined as the design matures, and will be finalized at the time that procurement specifications are issued. The PSA and RAM analyses will be used to confirm that these SSC performance goals are consistent with the overall pant safety and economic goals. One overall approach to the development of plant level performance goals is shown in Fig. 5-3.



Electric System Reliability Criteria
Electric System Generation Mix and Load Projections
Electric System Production Costing Models
Perform Sensitivity Analyses on Forced Outage Rates and Capacity Factors and Bus Bar cost for Specific Plant Sizes
Select Optimum Plant Configuration and define Associated levels of:
o Capacity Factor
o Forced Outage Rate
o Planned Outage Rate
o Generation cost (mils/Kw-hr)
Define plant level Production Goals
Define the Incremental Cost Curve for Plant Reliability (Forced Outage Rate) & Plant Capacity Factor
Estimate of Expected Reliability for each Plant Option
Estimate of Expected Availability for each Plant Option
Define Preliminary Set of Economic and Safety Goals
Projected Installed Costs for Each Plant Option
Basic Options for Plant Layout
o NSSS
o BOP
Historic and Projected estimates of Plant Reliability and Availability, CDF, CCFP and Risk
Confirm that selected goals do not violate any Regulatory or Societal Safety Standards
Estimate the Installed Costs for Selected Option
Estimate the CDF, CCFP and Risk for Selected Option
Plant Specific Severe Accident Cost Models
Calculate Economic Break-even Goals for CDF, CCFP and Risk
Select Appropriateand Cost Justified Plant Level Safety Goals

*FIG. 5-3. Development of plant level goals.*

### 5.4.1. Performance goals for generation

#### *5.4.1.1. Plant level goals (generation)*

Plant level goals are defined from a broad economic analysis and assurance that they comply with specific requirements which have been imposed by either the regulatory authorities or the owner. A description of one process which can be used to define these goals is provided below. However, as a practical matter, NSSS vendors and architect engineers generally provide a pre-certified or pre-licensed nuclear plant design package which implicitly, or explicitly, defines performance which is consistent with the generally accepted levels identified by the EPRI Utility Requirements Documents, the EUR or their equivalents used by other Member States.

In this particular situation, the options open to the plant owner may be limited to the selection, sizing and control philosophy at the component or major equipment level. The approach suggested and described in these guidelines does not presuppose any restrictions on the freedom of the plant owner to make choices, so that the full process can be described "in context".

The issues which have an important influence on the definition of high level plant performance goals lie both outside, and within, the scope of the basic plant design. Hardware design parameters (redundancy, diversity and operability) influence its reliability and capacity factor, but the generation mix, system size and system reliability criteria determine its economic worth. This means that to define the optimum plant reliability and capacity factor goals, it is necessary to be able to compare their incremental worth for each feasible option with the costs of achieving them. This is done by, first, examining the normally operating generation systems and defining the feasible plant configurations:

(a) NSSS size, type (BWR, PWR, number of loops), manufacturer and whether evolutionary or innovative;
(b) Nuclear power control philosophy (solid or liquid absorbers) and ability to quickly change power and run-back on loss of load;
(c) Main steam and energy conversion systems:
    - Turbine generator configuration, e.g. manufacturer, fast valving options, type of reheat, number of LP units,
    - Turbine bypass capability and the plant's ability to run in a self-sustaining mode following a load rejection or loss of electrical grid without SCRAM;
(d) The type of heat sink, e.g. run-of-river or cooling towers;
(e) Condensate and feedwater system, specifically:
    - Deaerator and system control margin which accommodate condensate and feedwater transients without feed-pump trip,
    - Heater drains and drain cooler configurations,
    - Number and types of condensate, condensate booster and main feedwater pumps (variable speed electric, turbine driven, etc.) and control philosophy (auto run-back, etc.),
    - Steam generator manufacture, design and type.

The expected reliability and capacity factor will be predicted for each basic design configuration, either by quantifying specially developed RAM models, or, by using a combination of expert opinion and historical information from similar plants.

An electrical grid system simulation model will provide the basis for a series of sensitivity analyses to predict the likely differences between annual and life cycle system operation. Because the system simulation uses the expected mix of generation, awaiting plant seasonal availability and efficiency and the predicted seasonal system demands it can provide good estimates of the relative benefits expected from each specific plant configuration. Since the costs of installing each option are generally well characterized, the optimal reliability and capacity factor can be determined from a comparison between averted outage costs and the costs of increased system reliability or availability.

Results from quantification of the RAM models for the selected design option become the candidate plant level performance goals.

The remaining issue is whether uncertainty in the point estimate values from the RAM analysis should influence selection of appropriate goals. Because it is generally appropriate to set goals which are challenging, provided they are feasible, it may be appropriate to select the final goal at the "one-sigma" level, i.e. one standard deviation above the mean value, because it should be feasible, and not far enough away from the mean to make it economically unjustified. The ultimate decision must be made by the owner, although the approach provided above will quickly move the decision into an area in which the technical and economic bases are well defined.

#### *5.4.1.2. System and major component goals*

The RAM model previously developed and quantified for the selected design option is used as the basis for a series of sensitivity analyses, in which each feasible change to plant systems and train is superimposed on the model to calculate its corresponding effect on plant reliability and capacity factor.

The costs associated with each change are compared to the benefits they return and an optimization algorithm is used to identify the least cost configuration which meets the overall plant level goals. This model becomes part of the preliminary design basis and the levels of performance assumed by the model become the basis for the system and sub-system performance goals. The uncertainty in each sub-system goal is used to guide their modification to make them feasible, yet challenging.

Figure 5-3 depicts one process which could be used to define the preliminary set of economic and safety goals for the ALWR.

### 5.4.2. Performance goals for safety

#### *5.4.2.1. Plant level goals (safety)*

The approach to selecting high level safety goals is similar to that used for performance goals, except that the level 1, 2 or 3 reliability models replace RAM models as the basic computational tool used in the goal setting process. The selected plant configuration, with the baseline safety system configuration provided by the NSSS vendor and Architect engineer, is used to construct the initial PSA (probably a level 1 or 1/2, defined to the subsystem level).

Following prediction of the baseline estimates of core damage frequency and confirmation that it is consistent with the plant's ability to meet applicable safety goals, the design optimization process begins. Within this optimization process, the design engineer uses the PSA to perform a series of high level sensitivity studies by modifying the reliability models to reflect various system configurations and success criteria and calculating the corresponding benefits, measured as changes in the predicted CDF, CCFP or large early release frequency (LERF).

When the magnitudes of the risk reductions which are predicted to occur as a result of various proposed changes to the plant baseline configurations are compared to their individual costs, an optimization strategy is used to identify the best overall configuration, i.e. the configuration which produces the greatest risk reduction from the baseline, at the minimum cost. This configuration becomes the basis for the new reference design after a detailed solution of this model has provided assurance that the plant is expected to comply with each prescribed safety goal.

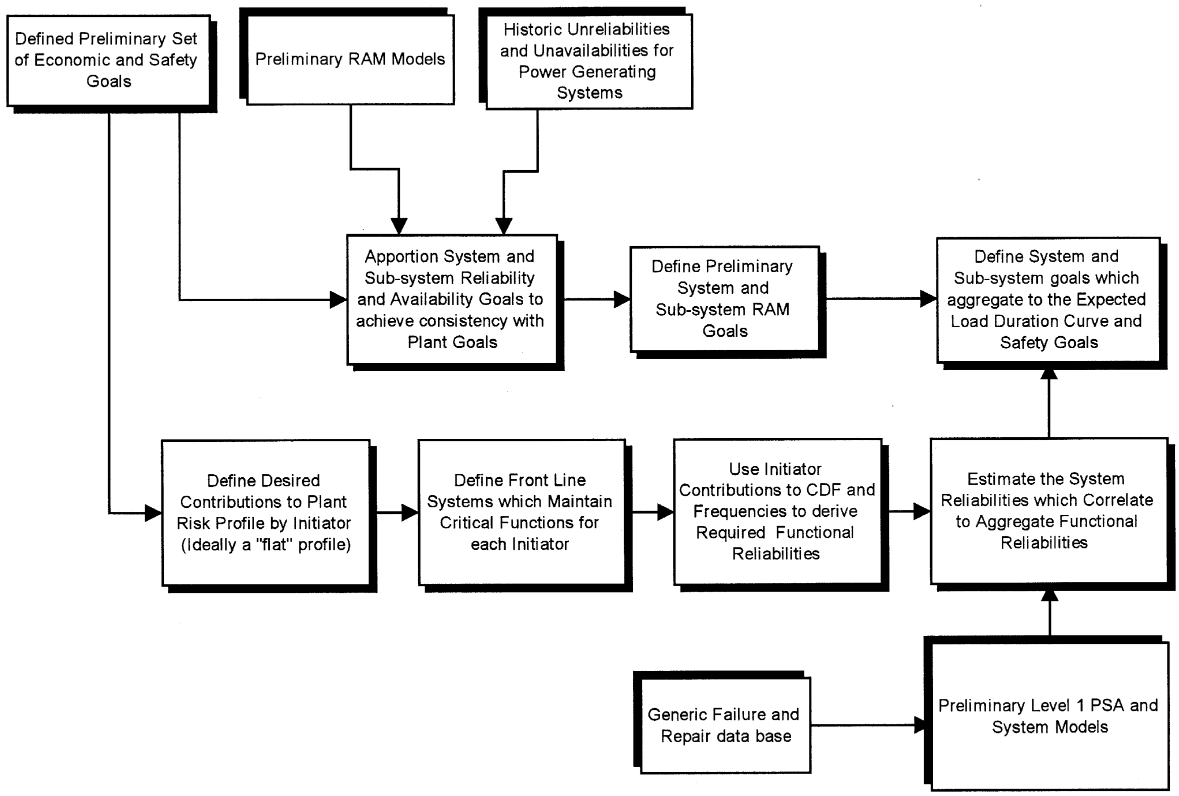
#### *5.4.2.2. System and major component goals (safety)*

The PSA is used to develop system level goals in much the same way that the RAM models were used for generation system goal setting, although in this case there is not only a desire to meet the prescribed goals but also try to define a design in which the individual contributors to risk are of the same magnitude, i.e. there are no dominant classes of contributors. A first approximation to this may result if the plant level goal is prorated amongst each initiating event category, and their frequencies and their overall contribution to the plant level goal used to define system or function level goals.

The PSA and cost models are then used to reapportion train and component reliability and unavailability to maintain the system level goals at its nominal value, while simultaneously evaluating total cost. An optimization algorithm will provide the first optimal solution which in turn will identify the preliminary set of system and component level goals and the preliminary design configuration, whose uncertainty will be used to adjust their single point values to levels which are both feasible and challenging.

Successful completion of this task will result in the definition of a baseline plant configuration and a set of front line system performance goals which can be used by the design team to further focus their efforts on achieving a design which exhibits the greatest degree of safety for the lowest possible cost. Performance goals for the support system infrastructure will be assigned later during the plant design process, however, the design team will again use the results and qualitative insights from the PSA to identify those support system structures and interconnections which preserve the defined front line system goals at minimum cost.

A process by which the preliminary system goals can be allocated for both generating and safety systems is shown in Fig. 5-4.



Defined Preliminary Set of Economic and Safety Goals
Preliminary RAM Models
Historic Unreliabilities and Unavailabilities for Power Generating Systems
Apportion System and Sub-system Reliability and Availability Goals to achieve consistency with Plant Goals
Define Preliminary System and Sub-system RAM Goals
Define System and Sub-system goals which aggregate to the Expected Load Duration Curve and Safety Goals
Define Desired Contributions to Plant Risk Profile by Initiator (Ideally a "flat" profile)
Define Front Line Systems which Maintain Critical Functions for each Initiator
Use Initiator Contributions to CDF and Frequencies to derive Required Functional Reliabilities
Estimate the System Reliabilities which Correlate to Aggregate Functional Reliabilities
Generic Failure and Repair data base
Preliminary Level 1 PSA and System Models

*FIG. 5-4. System goal allocation (preliminary).*

### 5.4.3. Optimization of the performance goals

The design team will exploit the capabilities of the preliminary RAM and PSA models, which have themselves evolved with the design, to identify the optimal SSC performance goals. In principle, this requires the goal setting team to:

- Perform sensitivity analyses to identify the potential worth, from improved plant generation or safety, for the range of feasible system "upgrades" or enhancements,
- Estimate the costs to achieving the reliability which would result from the implementation of each configuration used in the sensitivity analyses,
- Use the resultant system reliability-cost-benefit curves as input to an optimization algorithm to find the optimal plant configuration,
- Confirm that the resultant design meets all applicable design criteria and is suitable as the basis for the plant reference design,
- Calculate the default values for system reliability and availability and assign them to be the optimized plant performance goals,
- Incorporate the effects of uncertainty on the goals to ensure that they are challenging,
- Comparing the new design with past designs and the magnitude of the proposed goals with past operating experience, and use judgment to confirm the feasibility of the goals.

The generation and safety System goal Optimization process is shown in flow chart form by Fig. 5-5.

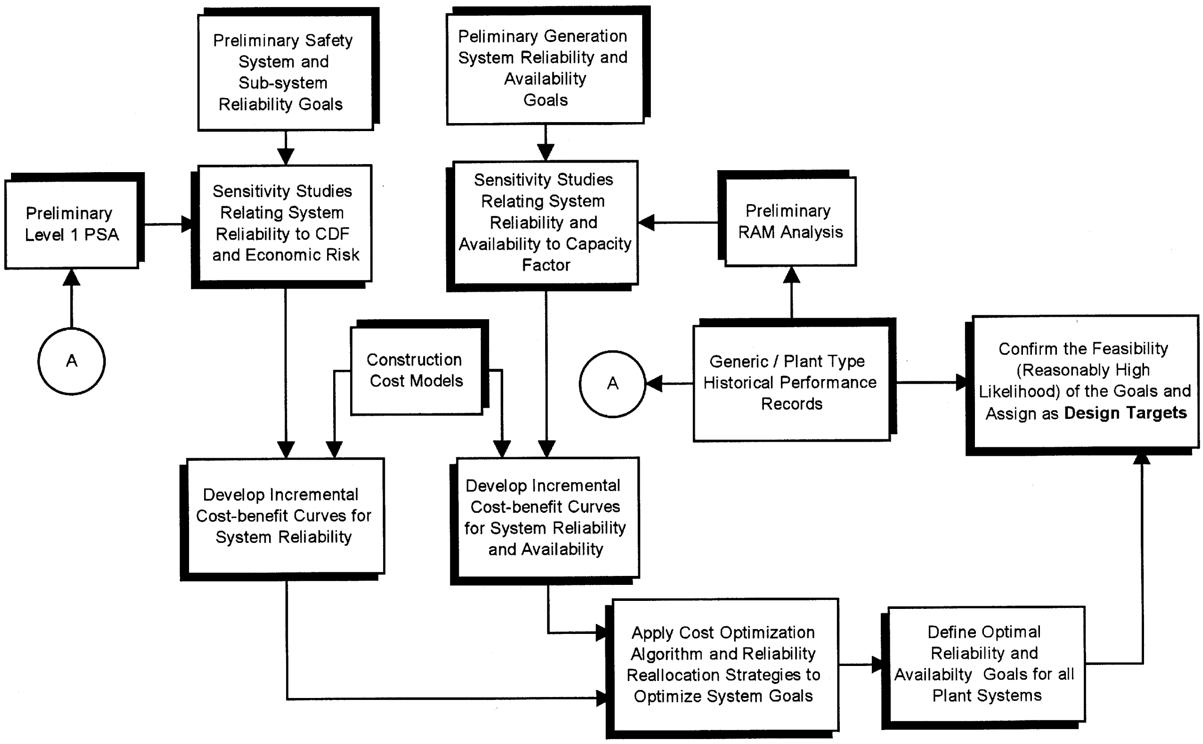

Preliminary Safety System and Sub-system Reliability Goals
Peliminary Generation System Reliability and Availability Goals
Preliminary Level 1 PSA
Sensitivity Studies Relating System Reliability to CDF and Economic Risk
Sensitivity Studies Relating System Reliability and Availability to Capacity Factor
Preliminary RAM Analysis
A
Construction Cost Models
A
Generic / Plant Type Historical Performance Records
Confirm the Feasibility (Reasonably High Likelihood) of the Goals and Assign as Design Targets
Develop Incremental Cost-benefit Curves for System Reliability
Develop Incremental Cost-benefit Curves for System Reliability and Availability
Apply Cost Optimization Algorithm and Reliability Reallocation Strategies to Optimize System Goals
Define Optimal Reliability and Availabilty Goals for all Plant Systems

*FIG. 5-5. System goals of optimization and allocation.*

## 5.5. ANALYTICAL MODELS

### 5.5.1. RAM models for D-RAP

The development of RAM models to support design decision making processes is necessary to provide an analytical process which can be us to provide initial assessments of whether the plant can be expected to meet its prescribed probabilistic production goals, where potential plant vulnerabilities may lie, and a tool which can be used routinely to predict the "worth" of each variously proposed design change, variation and enhancement in the optimization of the overall plant design.

The RAM models which will be needed to support the decision making process can be expected to include:

– Full forced outage rate predictor:
  - (i) Plant (un)reliability model which can predict the frequency of SCRAM or immediate plant shutdown, and identify the relative importance of each individual contributing SCRAM or shutdown scenario,
  - (ii) Plant maintainability model which predicts the expected plant outage duration, or, mean down time, for each dominant SCRAM or shutdown scenario,
  - (iii) Aggregation technique to calculate net contribution to unavailability,

– Equivalent availability predictor:
  - (i) Multi-state availability model to define the points on the cumulative distribution function for {probability of exceeding capability "X" vs. Capability "X"},
  - (ii) Integrator for CDF to calculate equivalent availability,

- Planned outage rate predictor:
  - (i) Scheduled test, inspection and maintenance requirements for planned outages,
  - (ii) Individual testability, inspectability and maintainability assessments for SSCs on critical path,
  - (iii) Aggregation technique to predict expected planned outage duration.

Any of the generally available analytical approaches can be used to meet these modeling needs although some are more efficient than others. The following are suggestions which are, by no means, intended to exclude other approaches. The general rule for selection of analytical methods and techniques is always the same-select a method which provides the requisite results for the smallest outlay of available resources. Familiarity with one particular approach, may in itself be sufficient justification for not wanting to use another method, even though in the long run, the second method may be faster. The decision is one of convenience, provided each method under consideration provides the required output, with the required degree of precision and uncertainty.

*Suggested or preferred modeling approaches*

Prediction of the expected levels of performance for a new, possibly untested configuration or design, necessarily places great reliance upon analytical approaches and methods, although actuarial information should still be used to provide a check of the analysis and to confirm that the results they are providing are both reasonable and practical.

*Reliability model for SCRAM rate prediction*

SCRAM reliability models are generally deductive models which include basic events, quantified in terms of their expected occurrence frequency (initiating events) or their conditional failure probability (sub-sequential of consequential failures). Solution of the model provides SCRAM frequency.

*Equivalent availability prediction*

Predictions of equivalent availability are best made with inductive models (event trees, GO models or truth tables) because they are most efficient when a spectrum of output states is possible. Whether the EA curve is defined from the results calculated for each feasible power states or from a limited set of predefined power states, depends upon both the precision desired in the answer and the cycle characteristics.

Event tree analysis can be used to identify the important discrete plant states which should be modeled, although, complete analysis with event trees may be complicated by tree size and the large number of possible end states. Reliability block diagram analysis is a very important part of generating systems analysis since it facilitates the construction of the plant power state matrix by breaking down the generation cycle/process into a series of independent functional or “series” elements, each with its own segment-specific success criteria.

### 5.5.2. PSA models for D-RAP

PSA models used to support D-RAP will follow the currently popular and effective computer aided methodologies. The only preferences should be in favor of enhanced applicability and ease of use in their applications. All methods provide acceptable results, and the characteristics of the plant will determine how much fidelity and precision is required in analyzing specific issues. This may particularly true when performing seismic and fire analyses, and whether a full fire and seismic PSA is required to meet the design team's needs or whether a less complicated seismic margins analysis or fire assessment.

Integration of the level 1 and 2 analyses should be of particular concern so that the costs of all proposed design changes in system redundancy and diversity or the reliability and maintainability of individual SSCs can be easily equated to their equivalent benefits from risk reduction.

The bibliography presented in Annex 1 can be used to provide guidance on the overall selection of approaches, although experience and internal resources will be an important determinant.

### 5.5.3. Economic models

The economic modeling process for generation losses use the standard set of utility economic assumptions described in Section 2. These are then used in combination with the equations shown below for each general class of unavailability. If the losses occur over multiple years, the equivalent present worth usually becomes the representative economic parameter to be used in the decision making process.

Individual categories and costs of generation losses from outages or degraded operation described by the load duration curve are described by the following:

**Planned outages**

Planned outages occur when the plant is shut down for refueling, modification or general inspection and the outage is planned well in advance when the seasonal system demands are minimum. The cost of lost generation from planned outages is calculated as follows:

$\$loss_{P.O} = MDC * P.O.\ hours/year * \$/MW/h_{Replacement}$

Where:

$\$loss_{P.O.}$= Annual cost of generation lost to planned outages
MDC = Plant maximum dependable capability in MW
P.O.= planned outage
$\$/MW/h_{P.O.}$ = Average differential cost of replacement energy supplied when the plant is shut down for refueling, modification or planned maintenance.

**Maintenance outages**

Maintenance outages occur as a result of equipment failures which do not require an immediate plant shutdown but can be deferred to the first week-end or period of low system generation demand when the cost of replacement energy can be reduced to a seasonal minimum.

The cost of lost generation from maintenance outages is calculated as follows:

$\$loss_{M.O} = MDC * M.O.\ hours/year * \$/MW/h_{Replacement}$

Where:

$\$loss_{M.O.}$ = Annual cost of generation lost to maintenance outages
MDC = Plant maximum dependable capability in MW
M.O. = Maintenance outage frequency
$\$/MW/h_{M.O}$ = Average differential cost of replacement energy supplied during maintenance outages.

**Full forced outages**

Full forced outages are incurred when a hardware or human failure results in an immediate plant shutdown (SCRAM or manual trip) or a controlled shutdown within twenty four hours. The economic impact from a forced outage is high because of the short time available to plan for contingency sources of generation to provide replacement energy from other generating facilities.

Because of the need to maintain spinning reserves and a capacity margin on the system to maintain electric system reliability, there may be additional capacity charges associated with forced outages. The cost of lost generation can be calculated as follows:

$\$loss_{F.O}$ = F.O. Freq. * Avg. hours/F.O. * MDC * $\$/MW/h_{F.O.}$
= SUM[FO1*MDT1, .... FOi*MDTi] * MDC * $\$/MW/h_{F.O.}$

Where:

$\$loss_{F.O.}$ = Annual cost of generation lost to full forced outages
F.O .= forced outage
Foi = ith occurrence of F.O.
MDTi = Duration of ith F.O.
MDC = Plant maximum dependable capability in MW
$\$/MW/h_{F.O.}$= Average differential cost of replacement energy supplied during forced outages.

**Partial forced outages or Forced reductions (F.R.)**

Forced reductions are incurred when a hardware or human failure results in an immediate reduction in plant capacity, but not a complete plant shutdown. The costs of lost Generation from forced reductions is calculated as follows:

$\$loss_{F\,R.}$ = SUM[FR1*MDT1*RC1, ... FRi*MDTi*RCi] $\$/MW/h_{F.R.}$

Where:

$\$loss_{F.R.}$ = Annual cost of generation lost to forced reductions
F.R .= Forced reduction
Fri = ith occurrence of F.R.
MDTi = Duration of ith F.R.
RCi = Magnitude of reduction in Capability for ith F.R.
$\$/MW/h_{F.R.}$ = Average differential cost of replacement energy supplied during forced reductions.

**Partial maintenance outages or maintenance reductions**

Maintenance reductions (M.R.) are incurred when a hardware or human failure results in a deferred reduction in plant capacity, but not a complete plant shutdown. The cost of lost generation from maintenance reductions is calculated as follows:

$\$loss_{M\,R}$ =SUM[MR1*MDT1*RC1, .. MRi*MDTi*RCi] * $/MW/h F.R.

Where:

$\$loss_{M.R.}$ = Annual cost of generation lost to maintenance reductions
M.R. = maintenance reduction
Mri = ith occurrence of M.R.
MDTi = Duration of ith M.R.
Rci = Magnitude of reduction in capability for ith M.R.
$\$/MW/h_{M.R.}$ = Average differential cost of replacement energy supplied during forced reductions.

**The plant capacity factor**

The plant capacity factor represents the percentage of the maximum possible generation (MDC*8760 h/a) which can be expected each year after the predicted losses to each of the sources described above are accounted for.

Specific risk based economic models must be constructed to assess the worth of changes to the plant which only influence safety, although there are some general approximations which can be used for preliminary screening, i.e.:

- Core damage frequency of 1E-05/a equates to an annual economic risk of $20,000 when only off-site consequences are considered (based on WASH-1400 results, and $1000/person-rem,
- Core damage frequency of 1E-05/a equates to an annual economic risk of $60,000 when both on- and off-site consequences are considered,
- A general bounding approximation to the equivalent present worth which is equivalent to these annual risks can be found by multiplying the annual economic risk by five. This is justified by assuming that the average annual risk is equal to the average annual leveled risk and the average plant fixed charge rate is 20%.

### 5.5.4. Reliability modeling issues

There are a number of issues which introduce unique difficulties into the reliability modeling process for advanced light water reactors. Some of the more important of these issues are briefly described in this section of the guide.

The reliability of active systems has been of primary importance to the safety of past reactor plant designs. The only influences on risk from passive failures came in the form of initiating events caused by process piping system pressure boundary failures or cabling problems which initiate reactor SCRAMs. Unless the passive failure was an initiating event, its contribution to overall system unreliability and concomitant risk was generally dwarfed by the contributions from independent and common cause failures of active components, so system level passive failures had little impact on plant risk.

The new designs of ALWRs, however, will have front line systems which are passive, meaning that they can operate independently from the plant support system infrastructure. These systems tend to be fluid-filled heat removal systems which maintain energy transport or transfer processes between the core and containment high energy sources and the ultimate environmental heat sink. Typically these passive systems use thermally induced pressure and density gradients to induce mass flow between the "hot" and "cold" ends of the system.

Though directly analogous to the failure modes seen in active cooling systems, passive system failure modes and their associated mechanisms tend to differ quite markedly. Examples of potential functional failure mechanisms for fluid energy transfer and transport processes in hydraulic or pneumatic systems, are described below:

(a) Loss of system integrity which initiates loss of fluid inventory, heat transport medium, and as a result causes:
  – Failure of the heat removal success path,
  – Loss of pressure control which may result in unfavorable conditions for effective heat transfer;

(b) Decreased system cleanliness which initiates an increase in system resistance, increased internal pressure drops and a reduction in the available thermo-dynamic driving head to a point that flow is inadequate. This can be caused by:
  – Increased roughness or cleanliness in piping systems which results in increased internal resistance to flow,
  – Full or partial blockages in the flow path which introduce pressure drops which reduce the available driving head to the point that flow is inadequate;

(c) Changes in end point, or heat sink, temperature changes which can potentially reduce the overall system temperature gradient, and:
  – Reduce the available driving head to the point that core and containment energy transfer or transport is inadequate;
  – Change the available density gradients which initiate or control make-up flow to a system, following a loss of its integrity;
  – change the available density gradients which initiate or control fluid mixing and affect their ability to transport neutron absorbers into the reactor core region to control reactivity;

(d) Changes in the cleanliness of heat transfer surfaces which reduce the effective heat transfer rate for the available temperature gradient.

The referenced fluids in these passive cooling systems may be gas or liquid, and are generally only of importance to nuclear safety systems. The process systems which play a role in electric generation will remain active, even in advanced reactor plants because there generally is no economic advantage to their having "fail-safe" characteristics.

When the failure characteristics for passive systems are translated into fault events whose occurrence frequency or conditional failure probability must be predicted to assess plant risk or the likelihood of an accident scenario, they fall outside the realm of most currently used databases. Confident prediction of the reliability of passive systems will be based on the extent to which several important parameters are understood:

- The frequency of catastrophic failure for nuclear piping systems which typically operate with single-phase flow;
- The probability that changes will occur in the thermodynamic and thermal-hydraulic parameters which are used to characterize fluid behavior in transient and steady-state simulations of system behavior.

An important characteristic of these influences on system reliability is that they are likely to be neither constant nor random but, very much a function of “ageing” or chronic degradation mechanisms and the plant operators’ ability to detect the progression of these mechanisms before they reach critical proportions. Before the designer can determine how to maximize the reliability of these passive components it will be necessary to understand:

- Failure mechanisms;
- Environmental and process conditions which influence the propagation rates for the identified mechanisms, e.g. stress, embrittlement, erosion-corrosion, pitting and fatigue;
- Environmental and process conditions during both normal and off-normal plant operating conditions, e.g. fluid temperature, pressure, velocity, pH, chemistry, electro-chemistry and potential impurities;
- Detection techniques, methods and thresholds for flaws, e.g. cracking and pitting, and chronic degradation, e.g. thinning, graphitization, hardening, and corrosive product build-up.

Since most of the information needed during the design process has a high technical and material specific content, it can only be generally referred to in this D-RAP guide. However, when the detectability of the passive failure is an important issue there are generic options available to the designer which should be considered as part of the D-RAP process.

#### *5.5.4.1. System inspectability*

The designer must define the expected inspection techniques which will be needed to detect important incipient faults and degradation in individual fluid systems and lay out the piping and vessels in a way which allows:

- Necessary access to perform the inspection for each expected technique (radiography, eddy current, ultrasonic, dye penetrant, etc.),
- Calibration pads which are accessible to the inspector (uninsulated, or easily removes insulation),
- Rigging, access and communication networks for remotely operated, or robotic, inspection equipment,
- Guard piping to divert pipe leakage into an area in which it can accumulate and increase the likelihood of reliable and timely detection-may be important if “leak before break” is credited in the prediction of the occurrence frequencies for pressure boundary failures,
- Inventory management systems which are capable of detecting leakage of the magnitude which is likely to provide forewarning of catastrophic failure,
- Coupons which match the materials of construction and weld characteristics and an ability to characterize their condition by providing surveillance capsules,
- Isolation and hydro-testing capabilities, and instrumentation if acoustic emission techniques are to be used to assess pressure boundary integrity.

### *5.5.4.2. System testability*

In addition to designing the system to be "inspectable" it is also important to design the system to be "testable". This requirement means that the designer should provide:

- Defined range of testing activities which will be needed to confirm complete functionality of the system and to detect any potential degradation in functional performance,
- Necessary boundary isolation capabilities for each part of the system which will be within the functional testing boundaries,
- Necessary instrumentation to monitor the necessary system parameters which are indicative of functional performance,
- Ready access, and system connections to energy sources (pneumatic, hydraulic) which may be needed to test system functionality, i.e. valve leakage or valve operation under accident loads,
- A feasible set of boundary conditions for the test which correspond to the conditions which are expected during an operational demand, i.e. conditions which are expected during a severe accident, if that is when the equipment will be demanded.

### *5.5.4.3. Predicting the reliability of passive systems*

To exploit the quantitative benefits from the analytical models which are at the core of D-RAP, it is necessary to not only understand the qualitative aspects of passive system reliability which are described above, but, also how these affect the predicted failure frequencies and probabilities:

- Frequencies for initiating events,
- Conditional probabilities for failure events which are sub-sequential or consequential to the initiator.

Of dominant concern to passive system reliability are predictions of the likelihood of:

- Piping failures which result in loss of fluid inventory which is greater than the normal make-up capability (LOCAs),
- System changes which change the internal resistance to flow,
- Environmental and process changes which affect the assumed boundary conditions for the system and the available thermal-hydraulic driving head for passive system flow,
- Failure of any human actions which may be needed to initiate or control system functions.

Because the probability of human failure is likely to be much higher than the probability of passive hardware failure, if human action or control is required for passive system operation, the human failure probability will dominate its unreliability. This implies that in a truly passive system, routine human intervention should be avoided wherever possible. Because the predicted failure rate for passive systems designs is expected to be very low with little, if any, actuarial data to support it for the specific boundary conditions which are expected, there may be a high degree of uncertainty in the value. This issue must also be considered when the PSA is used to guide design decisions.

Each of these contributions to passive system unreliability will be discussed briefly to identify the important issues, however, their resolution must be left to real design analyses when knowledge of the full circumstances dictate the level of analytical difficulty involved and indicate which analytical methods will provide the greatest returns for the resources expended.

It is important to recognize that as the ALWR exploits the benefits from the high reliabilities provided by passive systems, design failures and inadequacies will have an increased importance in the future.

### *5.5.4.4. Prediction of LOCA frequencies*

Two general methodological possibilities exist for prediction of the frequency for pressure boundary failure in a passive system:

- Analytical, in which convolution of the probability density functions for load and strength provides a distribution of its failure probability — failure only occurs when the load exceeds the strength;
- Actuarial, in which industrial experience from all sources is statistically analyzed to provide an overall prediction of the failure rate per standard section, weld or fitting. This actuarial data may be converted to a “correlation” such as the “Thomas correlation” so that the user can incorporate specific features and conditions into the overall prediction of failure rate to render it “plant-specific”.

In general, neither of these methods address time dependency of the failure rate. To incorporate the effects of ageing or chronic degradation mechanisms, a failure rate “acceleration factor” and the expected inspection efficiency and inspection schedule must be incorporated into the failure frequency predictions. This will probably be done in much the same way that the TIRGALEX database suggests (Reference NUREG/CR5510), and as discussed in the “ageing prediction” in Section 6.

Use of either the actuarial or analytical approaches will provide results which can be used to guide the prediction of risk, but, they alone may not be sufficient because of the high degree of uncertainty which may exist. This means that risk based system optimization may become subservient to demands for deterministic requirements which minimize the effects from LOCAs without any specific knowledge of the degree to which they are useful and the economic benefits they return. As a consequence the design team should:

(i) Use its expert knowledge and understanding of system specific influences on piping degradation rates to identify locations where internal system conditions result in the most severe local environments. These presumably will be the areas which are most prone to failure, so the design team should ensure that these most vulnerable locations are fully inspectable and testable;

(ii) Document this same expert knowledge of failure modes, mechanisms and flaw initiation and propagation rates in the plant design basis. During plant operation, this information will provide the means for prediction of degradation rates from inspection and test results and definition of a threshold of acceptability, so that the system maintainers can:

   - Understand where system degradation is likely to be the most severe,
   - Define “as new” and “acceptable” system condition,
   - Understand and interpret the importance of differences between “as is”, “as new” and “acceptable” conditions and determine where interventions is required to hold degradation rate to an acceptable rate,

  - Define a threshold of "unacceptability" for detected degradation,
  - Develop a strategy for risk controlled continued plant operation when a known degree of degradation is detected in a passive system;

(iii) Evaluate the potential benefits from the installation of leak detection systems, or other compensatory measures, in the pressure boundary locations of greatest vulnerability. This will be done whenever the PSA indicates that a dominant contribution to plant risk originates with assessments of the frequency for loss of system integrity, even after "leak before break" phenomena and associated intervention strategies have been;

(iv) Use nominal actuarial values for piping and vessel failure rates in combination with this expert understanding of failure modes, failure mechanisms and internal system conditions when it is necessary to develop an analytical estimate for the frequency or probability of a loss of system integrity.

The quantification process needed to calculate the probability of failure for a pressure boundary (P/B) will involve:

- Development of failure probability distributions for both the strength and loading of critical piping systems,
- using convolution techniques to calculate the intersect distribution which represent the probability that the P/B load will exceed the P/B strength and initiate P/B failure.

Development of the probabilistic load and strength distributions may require the use of probabilistic fracture mechanics codes, detailed knowledge of material properties, material integrity (flaw density and distribution), the dynamic loading of the P/B and both actuarial and analytically determined failure rates tempered with a measure of expert opinion.

#### *5.5.4.5. Prediction of passive system failure — non-LOCA induced*

When predicting the failure probability for non-LOCA induced passive system failures, i.e. those functional failures which are induced by causes other than system pressure boundary failure, it appears first necessary to understand the potential failure causes. Some of the more important causes are listed below:

- Chronic degradation mechanisms which increase internal system flow resistance or decreased heat transfer rates,
- Possibility of detection of degradation through tests and inspections and,
- How to develop a time dependent failure probability distribution for each of important non-geometric variable used in the thermal hydraulic system simulations and sensitivity analyses which constitute the safety and transient analysis and identify the required system success criteria.

From this information it should be possible to predict the failure probability for passive systems.

#### *5.5.4.6. Active SSC reliability*

There are many individual activities which can be initiated during the D-RAP process to influence SSC reliability. The rank-ordered list of SSCs will be key to limiting the expenditure of design resources to areas in which the payback is expected to be beneficial, so throughout the discussion below there is the presumption that the SSC list will be used to provide the necessary screening tool for inclusion of SSCs within each programme area. The resources expended in each area to enhance reliability will be strong function of its absolute importance to reliability, safety and economy. An indication of the scope of the SSC reliability investigation is provided by the simplified goal tree model shown in Fig. 5-6.

To maximize hardware reliability, there are several generic possibilities, each of which must be considered when deciding upon a D-RAP strategy for enhancement of the reliability for any specific SSC:

– Maximize the inherent reliability of the selected SSC by providing assurance that it is fully suited to the application under all normal, and off-normal, conditions. Generally, premature failure because of "design flaws" are the result of the designer selecting equipment which has:

  (a) Inadequate defenses against specific process influences or hostile conditions which affect the reliability of specific SSCs. This may be because the designer does not perform a reliability analysis for individual SSCs and conditions detrimental to reliable performance are not recognized at the time of equipment specification,
  (b) Little operating margin, so that it operates with a relatively high stress/load factor,
  (c) A very high service factor, resulting in operation with a high stress/load factor.

– Maximize the inherent reliability of the selected SSC by providing assurance that potential human errors and vulnerabilities in the operation, maintenance, repair and refurbishment processes do not result in premature failure. This occur when the designer selects equipment which has:

  (a) Poor operability characteristics which result in operational "error prone" situations. This typically occurs in control systems which require human input, but, either provide inadequate process information, or, have a time constant or frequency response which is incompatible with human capabilities,
  (b) Poor maintainability, characteristics so that either the required maintenance actions are very complex, required frequently, or are difficult to perform.

Each of these maintainability issues contributes to the probability that the maintainer will be placed in an error prone situation and perform inadequate maintenance which results in premature SSC failure.

– Maximize the reliability of the selected SSC by providing assurance that the number of unanticipated failures is minimized.

Generally, unanticipated failures result from:

(i) Inadequate diagnostic and monitoring instrumentation from which to infer SSC internal condition "on-line",
(ii) Lack of guidance in the interpretation of diagnostic and monitoring information and an inability to infer whether continued operation until the next planned outage is, or is not, advisable.

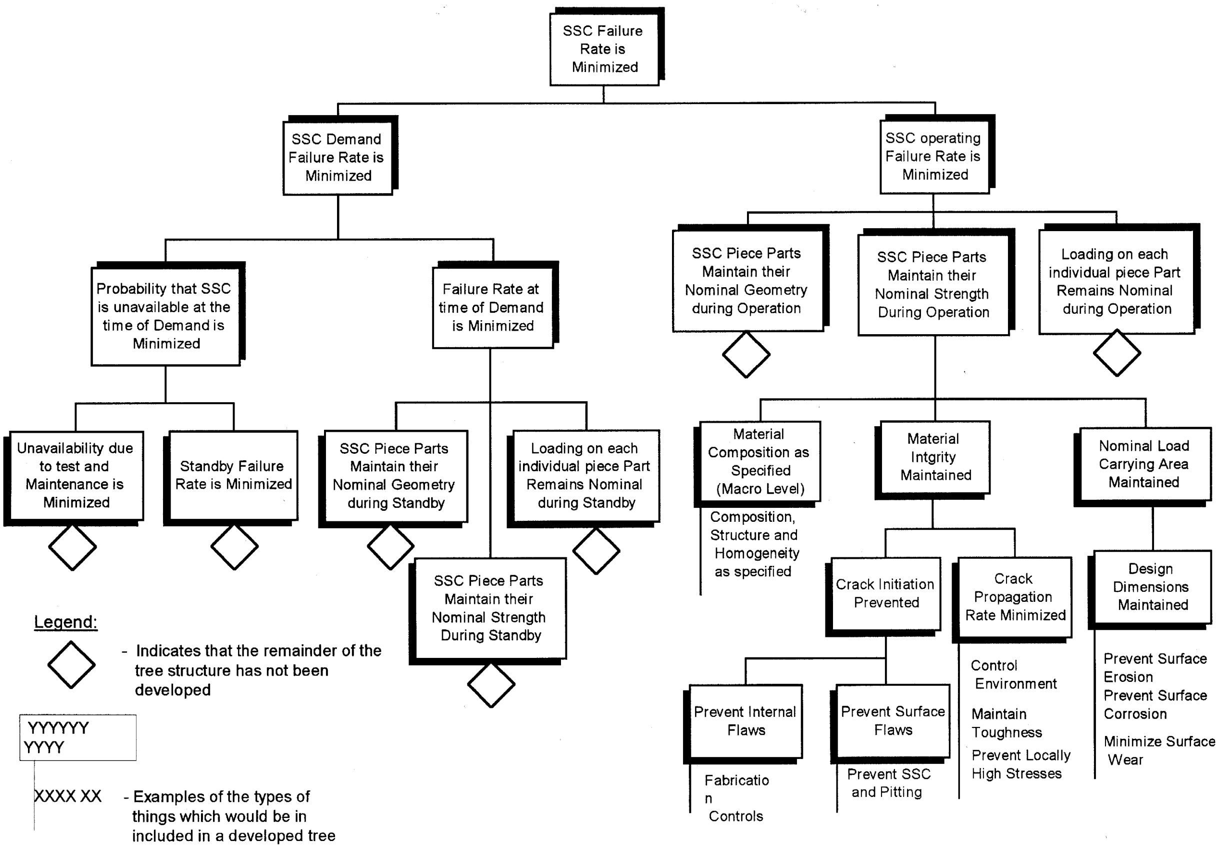

SSC Failure Rate is Minimized
SSC Demand Failure Rate is Minimized
SSC operating Failure Rate is Minimized
Probability that SSC is unavailable at the time of Demand is Minimized
Failure Rate at time of Demand is Minimized
SSC Piece Parts Maintain their Nominal Geometry during Operation
SSC Piece Parts Maintain their Nominal Strength During Operation
Loading on each individual piece Part Remains Nominal during Operation
Unavailability due to test and Maintenance is Minimized
Standby Failure Rate is Minimized
SSC Piece Parts Maintain their Nominal Geometry during Standby
Loading on each individual piece Part Remains Nominal during Standby
SSC Piece Parts Maintain their Nominal Strength During Standby
Material Composition as Specified (Macro Level)
Composition, Structure and Homogeneity as specified
Material Intgrity Maintained
Nominal Load Carrying Area Maintained
Crack Initiation Prevented
Crack Propagation Rate Minimized
Design Dimensions Maintained
Prevent Internal Flaws
Fabricatio n Controls
Prevent Surface Flaws
Prevent SSC and Pitting
Control Environment
Maintain Toughness
Prevent Locally High Stresses
Prevent Surface Erosion
Prevent Surface Corrosion
Minimize Surface Wear
Legend:
- Indicates that the remainder of the tree structure has not been developed
YYYYYY YYYY
XXXX XX
- Examples of the types of things which would be in included in a developed tree

*FIG. 5-6. Contributors to SSC unavailability — failure rate.*

The D-RAP must formally address each of these issues for important SSCs and incorporate reliability assessment into the design and selection process for SSCs. To prevent all of the above from contributing to premature SSC failure when the plant goes into operation, the designer must understand:

– The functional demands which will be made of the SSC, its operational profile and operating environment,
– Which failure modes and mechanisms are expected to be important during each mode of operation (SSC characterization),
– How design and selection of the equipment can exploit "built-in" defenses against important failure modes and mechanisms,
– How to recognize and diagnose the effects of flaw initiation and propagation from damage state to damage state to facilitate timely intervention before functional failure occurs.

This leads to the requirements for a formal reliability evaluation of each important SSC which will provide a technical basis for the D-RAP team's being able to develop:

– An appropriate set of performance specifications and requirements for each SSC which ensures that the proposals which are received from prospective vendors to supply the requested equipment will:
  (i) Demonstrate that the equipment is suitable for its proposed application, i.e. is manufactured from process-compatible materials and designed with adequate margin,

(ii) Demonstrate that it can meet all specified reliability criteria, which are commensurate with its importance to reliability, safety and economy,

(iii) Contain sufficiently detailed information for the D-RAP design team to independently predict its expected reliability;

- An effective method which can be used by the D-RAP design team to evaluate the relative and absolute reliability and maintainability for each vendor's offering of important SSCs;
- A system and equipment design which ensures that installed diagnostic and monitoring instrumentation is adequate and effective, and a process which assures its implementation.

This same evaluation process will lead to an examination of maintainability requirements for important SSCs to ensure that it does not have an adverse effect on maintainer error rate. This maintainability review should focus on the maintenance and repair processes and whether they are:

- unnecessarily complex,
- required on an unnecessarily frequent basis.

### 5.6. IMPORTANCE MEASURES AND PERFORMANCE INDICATORS

The products which result from the goal setting process will include both simplified RAM and level 1 PSA models whose structures match the selected "optimal" configurations. The next step in the D-RAP process is one of identifying the absolute and relative importance of each SSC so that the design, specification, procurement, manufacturing and installation processes can be focused on either preserving or enhancing the inherent reliability and availability levels of the hardware, wherever justified:

- Initially, these measures of importance should be consistent with the system performance goals, but, as the design matures the designer teams focus will shift towards assuring the optimum level of reliability, availability and maintainability for all SSCs,
- For those SSCs which have low importance to generation and safety, normal industrial practices and commercial quality will likely be adequate,
- For other, more important SSCs, the imposition of requirements by the quality and reliability assurance programmes will be commensurate with their importance.

However, it must also be remembered that the design must always comply with all deterministic regulatory requirements, unless they have been overtly waived by the cognizant regulatory authorities. Enhancements and design changes suggested by analytical insights provided by the D-RAP must always be secondary to legal constraints or other commitments which are self-imposed upon the design, e.g. by an owner's commitment to comply with the Utility Requirements Document, the European User's Documents, or other industry codes, standards or industrial "good practices".

The design team must either accept these constraints "as is" or use insights from the formal D-RAP process to generate a technically honest and sound foundation for arguments which elicit their waiver.

The real strength of the RA programme comes from its ability to fulfill this role from the inception of the design, when there remains time to initiate requests for waivers to the licensing basis for the plant without their having an important negative impact on project schedule or cost.

The key to programme success, however, lies with the development of a rank ordered list of SSCs and a list of all important common cause failures, human actions and initiating events. These lists can then be used to guide the application of RAP, and prioritize the imposition of more stringent requirements wherever they are justified.

This rank ordering process for RAP will be based on SSC, event or component "importance", generally measured as the sensitivity of the outcome (core damage frequency, capacity factor, SCRAM rate, etc.) to the failure probability of each component, human action or common cause failure.

### 5.6.1. SSC importance to safety and economy

Characterization of the importance of component performance to plant safety can usually be done easily because the PSA produces clear relationships between transient conditions and failure events and their resulting in a possible outcome which affects safety, e.g. core damage, containment failure given core damage, or, exposure of the plant staff and general public to radio-isotopes because of containment failure and subsequent release of fission products to the environment. Tight linkage between the failure of individual SSCs and this limited set of important plant outcomes implies that there may be a limited set of measures which can be used to infer component importance.

When calculating safety importance measures for SSCs, core damage frequency is usually the surrogate value for "safety". This is primarily because of the difficulty in calculating the importance measures for level 2 PSA states when there is often incomplete coupling between the level 1 and level 2 analyses and accident sequence cutsets are not explicitly necessarily carried through to their natural and unique conclusion.

Until PSA level 2 and 3 analyses are fully integrated, direct estimation of the ratio between a change in the reliability or availability of an individual SSC and its effect on source term frequencies or risk is very difficult. Currently, this coupling can only be achieved by extrapolation with risk impact curves, in a manner similar to that proposed in "Measures of Risk importance and their Applications", NUREG/CR-3385, written by W.E. Vesely, et al.

Assessing the importance of individual SSCs to generation and production economy is complicated by the large number of possible plant states which represent success, e.g. the complete spectrum of success states which exist between minimum load and full power. This raises the question as to which benchmark should be used since SSC importance depends not only on its reliability, but also upon the magnitude of the effects that its failure has on plant operation, i.e. whether its failure results in a full forced outage, SCRAM, or a partial forced reduction. In practice, a combination of measures with some form of compensation or weighting factor will be needed.

### 5.6.2. Importance of SSCs and their failure modes

Because the PSA uses the probability and frequency of individual failure events to synthesize plant level accident frequencies, it is important to combine importance contributions from all individual failure events (failure modes) when assessing overall SSC importance. The importance of individual failure modes must still be retained, because this information is needed to identify the important functional failure modes for the SSC. Figure 5-7 provides an overview of one process for using importance measures to rank individual SSCs and how the combined characteristics of each importance measure can provide additional information to guide the application of specific D-RAP activities.

Though the primary value of D-RAP comes from its ability to focus attention on the real issues which are important to safety, application of RAP principles also plays a critical role in assuring that there are no insidious oversights, i.e. RAP augments the role played by the quality assurance programme by strengthening the design team's management systems and preventing errors and oversights from creeping into the design. Though it is almost certain that the design review process, construction inspections and pre-operational testing programmes will uncover any important design errors or oversights before the plant goes into operation, their correction during start-up or operation may have a very important impact on cost, either in terms of:

- Direct costs, associated with correction of the physical plant to remedy the effects of the oversight or error,
- Indirect costs associated with the implementation of increasing levels of inspection and administrative control which inevitably seem to follow the discovery of a failure in a management system. This latter contributor to cost is often hidden, yet ultimately it often results in an additional administrative burden which impacts every aspect of plant design, construction and operation.

RAP influences the development and implementation of management systems which force designers to "pay attention to detail" during the performance of every activity which influences the reliability, availability or maintainability of each important design element. The ranked list of SSCs is one of the most important tools used to guide RAP, because it is this list which helps to identify the areas in which the design team should pay particular attention to each of the issues discussed above. The question next is how to identify and rank these SSCs and to understand how the many different "importance measures" can be used to do so effectively.

### 5.6.3. Importance measures

There are a number of quantitative importance measures which are routinely produced by the computational software used by reliability engineers to perform systems analyses, RAM and risk assessments. These numerical importance measures allow the analysts to rank individual contributors to the basis of their overall contributions to unreliability or risk.

Because importance measures differ from each other and produce different insights about why individual SSCs are important, a brief description of their functional nature is provided. An understanding of their similarities and differences can be exploited when characterizing SSC "importance", i.e. whether the numerical importance values for an individual SSC are functions of its reliability, availability or maintainability.

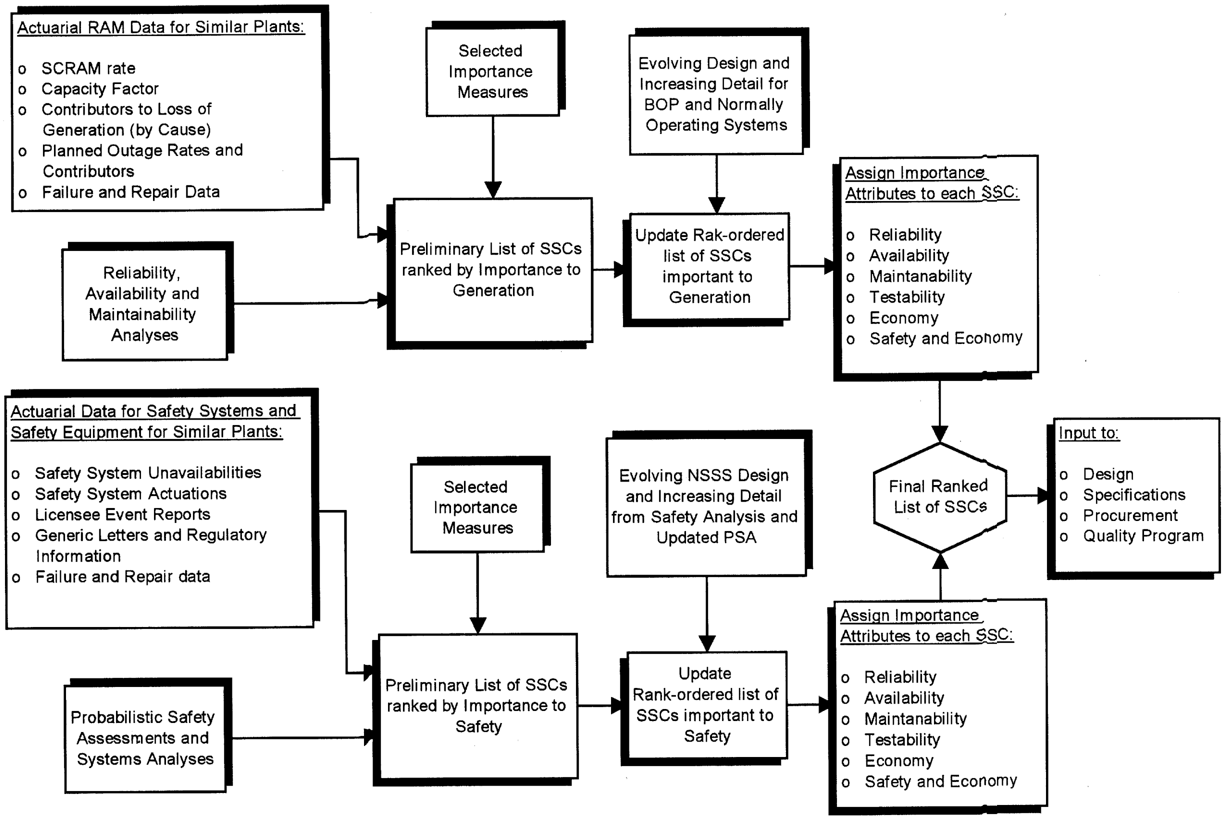

Actuarial RAM Data for Similar Plants:
o SCRAM rate
o Capacity Factor
o Contributors to Loss of Generation (by Cause)
o Planned Outage Rates and Contributors
o Failure and Repair Data
Selected Importance Measures
Evolving Design and Increasing Detail for BOP and Normally Operating Systems
Assign Importance Attributes to each SSC:
o Reliability
o Availability
o Maintanability
o Testability
o Economy
o Safety and Economy
Reliability, Availability and Maintainability Analyses
Preliminary List of SSCs ranked by Importance to Generation
Update Rak-ordered list of SSCs important to Generation
Actuarial Data for Safety Systems and Safety Equipment for Similar Plants:
o Safety System Unavailabilities
o Safety System Actuations
o Licensee Event Reports
o Generic Letters and Regulatory Information
o Failure and Repair data
Selected Importance Measures
Evolving NSSS Design and Increasing Detail from Safety Analysis and Updated PSA
Final Ranked List of SSCs
Input to:
o Design
o Specifications
o Procurement
o Quality Program
Assign Importance Attributes to each SSC:
o Reliability
o Availability
o Maintanability
o Testability
o Economy
o Safety and Economy
Probabilistic Safety Assessments and Systems Analyses
Preliminary List of SSCs ranked by Importance to Safety
Update Rank-ordered list of SSCs important to Safety

*FIG. 5-7. Importance measures and ranking SSCs.*

*$R_o$ = Present risk level,*
*$R_i^+$ = Increased risk without feature I, or with feature I assumed failed,*
*(Cutset frequency with component I assumed to be completely failed),*
*$R_i^-$ = Increased risk with feature I optimized, or with feature I assumed perfectly reliable,*
*(Cutset frequency with component I assumed to be working perfectly),*
*$A_i$ = Risk achievement worth of feature I,*
*$D_i$ = Risk reduction worth of feature I,*
*$I_i$ = Fussel-Vesely importance of feature I,*
*$\Delta_I$ = Birnbaum, or the reliability importance of feature I.*

Each importance measure which is typically used to characterize the results and insights from reliability assessments is described briefly below, together with an interpretation of its own unique, and practical, qualities which assist in guiding the activities which are part of a reliability assurance programme. The source for this material can generally be found in "Measures of Risk Importance and their Applications", NUREG/CR-3385, authored by W.E. Vesely et al.

### Fussel-Vesely Importance measure

Definition: The fractional contribution of component I to the risk, or the risk reduction worth on a ratio scale.

$I_i = (R_o – R_i^-)/R_o = (D_i – 1)/D_i$

*Insights and applications:*

- Fussel-Vesely importance provides a general estimate of the relative importance of a failure event/component which is based on the accident sequences in which it plays a role, and their fractional contribution to overall core damage frequency or risk.

**Risk achievement worth (RAW)**

Definition: The increase in risk if the component were to be removed, failed or made completely unreliable.

$A_i = R_i^+/R_o$ (ratio scale)
or, $A_i = R_i^+ – R_o$ (interval scale)

*Insights and applications*:

- Since the conditions imposed by the importance measure mimic those which occur when a component is taken out of service for maintenance, the importance measure can reflect the importance of component maintainability,
- Components which have inherently high levels of reliability will indicate high RAW and likely promise low returns from an improvement in their availability or reliability.

**Risk reduction worth (RRW)**

Definition: The decrease in risk if the feature were assumed to be optimized or made perfectly reliable.

$D_i = R_{0/}R_i^-$ (ratio scale)
or,$D_i = R_{0\,–}R_i^-$ (interval scale)

*Applications and insights:*

- Identifies components which promise the greatest returns from an improvement in their reliability or availability.

**Birnbaum importance**

Definition: The change in system reliability as a function of the change in component reliability.

$\Delta_I = R_i^+ – R_i^- = A_i + D_i$

*Applications and insights:*

- Because the Birnbaum importance measure is the sum of the risk achievement and risk reduction worth of component I on an interval scale, it is generally felt to convey less information than each of its individual constituent measures, however:

(a) Because the Birnbaum importance measure is a function of system reliability structure, not of the reliabilities of individual components, it can be very valuable in focusing the designers’ attention on areas where changing levels of redundancy should be evaluated,

(b) In a series system, the sum of the Birnbaum importances for each component is equal to the Birnbaum importance for the system, and provides a measure of the change in risk that is associated with system failure.

When risk is measured as CDF, the Birnbaum importance for a system is equal to the conditional probability of core damage following system failure.

- When the Birnbaum importance of system failure is combined with the probability of pipe failure, it can provide a “weld inspection” measure of importance because it can be interpreted to be an approximation to the core melt risk caused by system/component failures caused by pipe failures. This measure could be important when assessing the importance of passive system components in ALWRs.

These particular insights are drawn from “Feasibility of Developing Risk-Based Ranking of Pressure Boundary Systems for In-service inspection”, NUREG/CR-6151, authored by T.V.Vo et al.

**Increased and decreased failure probabilities**

There are two additional importance measures which are similar in character to the RAW and RRW. However, instead of relating the overall change in reliability to an assumption of complete success or failure of an SSC, a more moderate increase or decrease in probability is assumed.

In this case, the importance measures are defined and calculated as follows:

$I = \{f(b`) - f(b)\}/f(b)$
or,
$I = \{f(b) - f(b``)\}/f(b)$

Where:

- The failure probability of the item under consideration increases from b to b`,
- The core damage frequency, f(b), increases to f(b`) as the item’s failure probability increases from b to b`,
- The failure probability of the item under consideration decreases from b to b``,
- The core damage frequency, f(b), decreases to f(b``) as the item’s failure probability decreases from b to b``.

The resultant importance measures provide the ratios between a change in basic event reliability or availability and the resultant change in core damage frequency, over a range of values which are typically encountered during plant operation. This may provide a good measure of importance to RAP, although RAW and RRW bound the situation and prevent inadvertent omission of important SSCs because the selected ranges for b` and b`` were inappropriate.

### 5.6.4. Interpretation of importance measures to rank safety systems

It is important to understand the underlying physical relationships within these importance measures so that they can be used to maximum effectiveness in a D-RAP. Because SSC importance is key to providing the focus needed by the design team, as it searches for the areas where potential improvements promise the greatest returns, it is essential that team members have a pragmatic understanding of their meanings.

The insights provided by these importance assessments also tell the design team where they must use “safety grade” equipment or where reliance upon industrial “best practices and commercial quality products” are adequate. This approach towards “graded QA” provides assurance that the “less important” SSCs can be provided with requisite levels of reliability and availability at very competitive costs.

One scheme has been put forward by the US Nuclear Energy Institute in their document entitled “industry guideline for Monitoring the Effectiveness of maintenance at Nuclear Power Plants” (NUMARC 93-01) in which the Institute suggests the use Fussell-Vesely and risk achievement worth Importance measures to rank the importance of SSCs, specifically in light of maintenance activities, as follows:

Screen #1:

- Rank all SSCs in decreasing order, by RRW,
- Eliminate RRWs which are unrelated to maintenance,
- Normalize each SSC RRW by the sum of all RRWs related to maintenance,
- Consider all SSCs that contribute 99% to the sum of risk reduction importances as “risk significant”.

Screen #2:

- Consider each SSC which has an RRW which is greater than 1.005 (RRW exceeds 0.5% of CDF) to be “risk significant”.

Screen #3:

- Consider each SSC to be “risk significant” if it is included in cutsets, ranked in decreasing order, which cumulatively account for 90% of the contributions to core damage frequency.

Screen #4:

- Consider each SSC to be “risk significant” if its risk achievement worth shows at least a doubling of core damage frequency.

A more detailed approach is suggested by “Evaluations and Utilizations of Risk Importances”, NUREG/CR-4377, authored by W.E. Vesely. In this model, the area bounded by the system RAW importance measure, plotted on the ordinate axis, and the system F-V importance measure, plotted on the abscissa, is divided into four quadrants. The axes for the quadrant separators are drawn where the F-V importance is equal to 5E-3 and the RAW is equal to 2.

Where the plots of F-V and RAW importances for a specific system fall within the boundaries of this segmented diagram will determine how it can be categorized within the context of the following definitions:

Where the SSC has an important influence on the potential for risk reduction, the goal should be to:

- Make the present risk lower,
- Receive the most attention in the search for potential enhancements (system modifications).

Where the SSC has an important influence on the potential for safety assurance, the goal should be to:

- Assure that risk does not increase;
- Protect against deterioration in performance (enhanced maintenance and maintainability and minimized out-of-service time).

The plots of F-V and RAW importances for individual SSCs into the four quadrant model can be interpreted as follows:

Upper right quadrant (RAW>2 “AND” F-V>5E-3),
– Significant impact on risk reduction and safety assurance.

Lower right quadrant (RAW<2 “AND” F-V>5E-3),
– Significant impact on risk reduction.

Upper left quadrant (RAW>2 “AND” F-V<5E-3),
– Significant impact on safety assurance.

Lower left quadrant (RAW<2 “AND” F-V<5E-3),
– Insignificant impact on risk reduction and safety assurance.

A graphical interpretation of this approach is provided in Fig. 5-8. The actual boundaries were suggested by NEI’s document, NUMARC 93-01.

It is important to understand the relationships between level 1 and level 2 PSA importances. Unless the containment performance assessment is coupled directly to the level 1, it may be necessary to make a separate calculation of component importance to release category. For example, the “large early” release category is of primary importance to risk, so to find component importance to risk, it may be necessary to calculate component importance only on the basis of the sequences which result in LERF, not on the basis of all of the sequences which result in core damage.

### 5.6.5. Assignment of failure modes for each SSC

In addition to estimating the importance for each SSC it is also important to provide additional insights as to which SSC characteristics influence this importance to guide the designer in developing design and procurement specifications which minimize the impact from the most important failure modes and guide the imposition of quality assurance requirements. This information is particularly important to a graded QA programme where additional flexibility in the quality requirements can lead to significant cost savings.

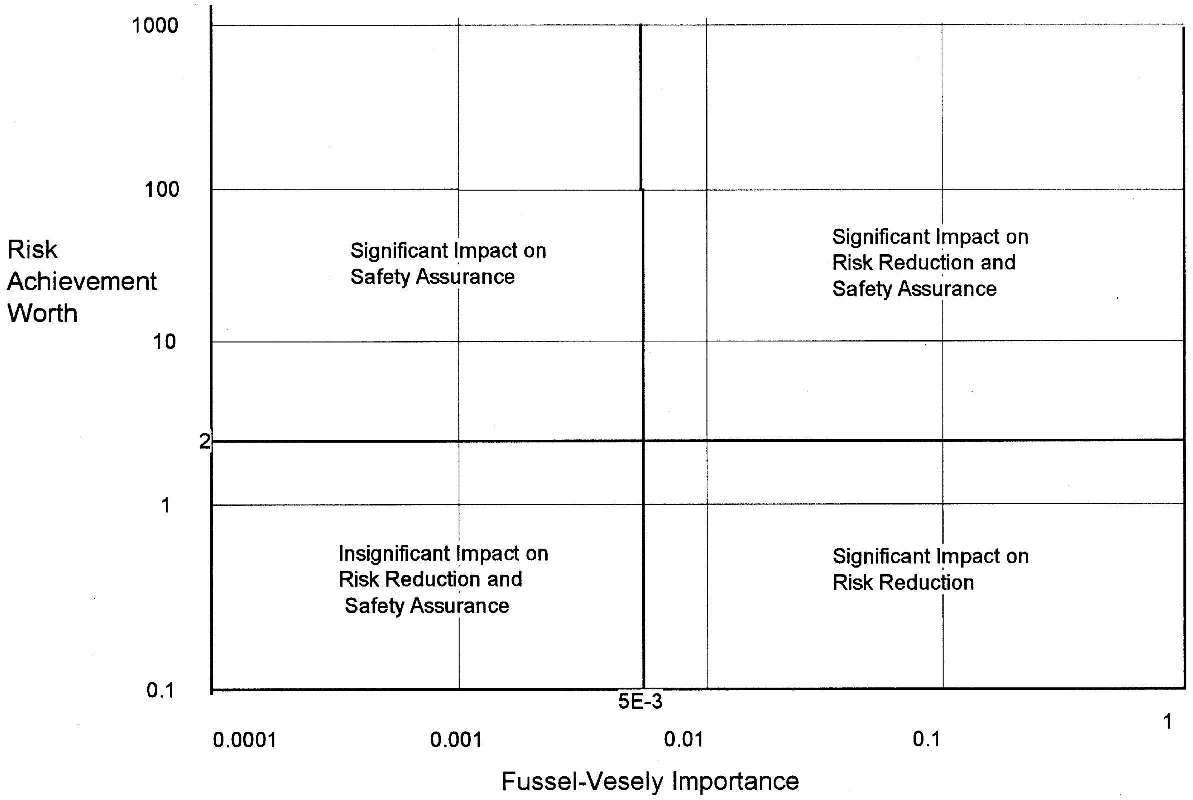


*FIG. 5-8. Use of importance measures to categorize SSCs.*

Identification of the most important failure modes will be derived from two primary sources:

– Detailed low-level failure modes explicitly included in the PSA or RAM models. Where individual detailed failure modes are included in the models, direct estimates of their individual importances and their dominant functional failure mode can be made from the PSA and RAM study results;

– High level functional failure modes explicitly included in the PSA or RAM models. Where the PSA and RAM models only include high level functional failure modes, the importance of individual contributors can be derived from:

(a) Databases which show the percentage contribution that each makes to overall reliability and availability (EPRI-2032);
Where there is only an inexact correspondence between the database and the proposed design hardware, expert judgement may be required to provide the requisite level of detailed importance estimates.

(b) Failure Mode and Effects analyses (FMEA).
In this case, an inductive failure analysis (what happens... if... fails?) is conducted for the SSC to identify each possible functional failures mode. Following their identification, their relative importance can be estimated by expert opinion which has been calibrated with specific, but necessarily limited, operational data.

### 5.6.6. Performance indicators

Detailed descriptions of SSC importance measures and their applications were provided because of their value in providing a reliability focus to the design team and assuring that resources used to enhance the design are used where the expected payback is the greatest. To determine how effectively each D-RAP contributes to this objective, a set of “performance indicators” can be used. Periodic analysis of these indicators can both identify and diagnose management systems weaknesses, to identify trends provide feedback on how effective past changes have been.

High level plant RAP performance indicators cannot be completely defined until the RA programmes are defined for an individual plant project organization, although the topic is addressed in the O-RAP description (Section 6) at some length because some management indicators are generic to all generating plants. Within D-RAP there may be generic management system indicators, although care must be taken when using an indicator which does not have a clearly defined foundation. For example, an increasing trend in the “number of design changes/period” can be interpreted both positively and negatively. In a negative sense it may indicate poor initial decision making by the design team, whereas in a positive sense it can reflect the effectiveness of RAP’s ability to find and cure a large number of problems early in the design phase.

The power of the functional hierarchy contained within a “goal tree” provides one particular approach which may be useful in defining effective performance indicators, although frequently in practice their definition results from the combined wisdom and experience of the design or plant management teams.

The primary source of information which is available to guide the use of goal tree analysis in the definition of performance indicators, is contained in the “Integrated Approach Methodology: A Handbook for Power Plant Assessment”, (Sandia Report, SAND87-7138). There is an additional discussion of the topic in Modarres’ book, “What Every Engineer Should Know About Risk and Reliability Analysis”. Briefly, in constructing a goal tree, the analyst takes the following steps:

- Define the objective for the management system, both singularly and unambiguously,
- Construct the hierarchy of sub-goals which must be achieved if the defined overall objective is to be satisfied,
- Review each sub-goal and ask the question, “what information provides evidence of its success or failure?” This becomes one of the many elements in the set of information pieces which are candidates for inclusion as “performance indicators”,
- Select information which is available to indicate success or failure of the highest level goals as the candidate performance indicators for the specific programme,
- Repeat the process for each important management system,
- Compare the incremental costs of collecting and analyzing the information for each set of performance indicators with its expected benefits and identify the final list of performance indicators to be monitored during D-RAP.

### 5.7. THE MASTER PLANT LIST OF RANKED SSCs

The models and results from the PSA and RAM analyses will be used to identify the preliminary list of SSCs. Though a single list may be desirable, as a practical matter the D-RAP will probably provide at least two lists of SSCs, one for safety and one for economy. Generally there is overlap where important contributors to the plant SCRAM rate are important to lost generation and safety because they are potential accident initiating events.

At the inception of D-RAP the analytical PSA and RAM models will be coarse and lacking in explicit detail, so reliance will be placed upon actuarial data to provide the initial basis for SSC ordering. As the design matures and the detailed design evolves, analytical models will increase in detail and fidelity to the final design, and as a result, provide greater insights through the calculated importance measures. Ideally the results will be in the form of:

- Overall importance to safety, i.e. provide a measure of the effect of individual SSC reliability or availability on core damage frequency, or if possible, additional risk measures which can be related to the prescribed plant safety goals and economic risk.
- A plot of "risk reduction" vs. "safety assurance" to assist in categorization of SSCs.
- Overall importance to economy, i.e. provide a measure of the effect of individual SSC reliability or availability on capacity factor, and if possible, equivalent economic factors.
- Identification of a set of attributes for each SSC which provides a fairly complete, yet abbreviated, characterization of SSC importance:
  - (i) Failure has an effect on both safety and economy,
  - (ii) Functional failure modes which are of greatest importance,
  - (iii) Indication of whether SSC failure mode importance is a function of its reliability, availability or maintainability.

The list of SSCs will be used by the design team to provide the basis for focusing resources and efforts in areas which promise the greatest positive return in the form of enhanced safety or economy.

The ranked list of SSCs will provide a "living" basis for design importance, meaning that the positioning of individual SSCs will be fluid. As the design matures and the design team's analytical tools increase in detail and fidelity, new issues will arise, new items will be added to the SSC list and the positions of existing SSCs on the list will be changed to reflect their new relative importance.

**External initiating events and importance of SSCs**

Because the structural default of the plant may not be finalized, the initial rank ordered list of SSCs will probably not include the effects of fires, internal floods nor external events, in particular seismic, external floods and severe weather. However, as the design matures, and the details become better defined, the PSA will be extended to include the effects of these external initiating events and the rank-ordered list of components which are important to safety will be reassessed. The results from this reordered list will be used to guide the SSC specification and procurement process.

The design team must always ensure that all SSCs meet appropriate regulatory and industry requirements, but, where discretionary changes to replace or augment deterministic requirements are indicated, the focus of the design, specifications, procurement and quality requirements of individual items will be guided by numerical screening criteria, individual SSC importance measures and the individual attributes assigned to each SSC.

## 5.8. DATABASES FOR D-RAP

### 5.8.1. The D-RAP plant hardware database

The ability to perform quantitative reliability analyses to predict the performance of a new nuclear generating power plant depends very much upon the ability of the reliability analyst to both produce a mathematical analog to the plant which accurately relates hardware and human performance to the overall plant objectives, and to identify appropriate performance characteristics for these human and hardware failure events.

In combination, logic models and the quantitative estimates of failure frequencies or conditional failure probabilities for human actions and hardware components can be used to synthesize an overall prediction of future plant performance. The set of human and hardware performance parameters used to quantify the PSA and RAM models are normally referred to as the "plant database".

#### *5.8.1.1. Potential data source*

There are many diverse sources of data, some public, some proprietary. Generally they are of the following types:

- Industry generic databases,
- Company generic databases,
- Sister plant generic databases,
- Plant specific data.

The types of data or failure information which are needed to convert hardware failure information into failure rates and failure probabilities suitable for use in a PSA or RAM analysis are related to the two kinds of equipment typically encountered in a nuclear plant:

- Continuously operating (repairable) equipment:
  (i) when it fails, it causes a process upset condition,
  (ii) when it is repaired the process can be restarted,
- Standby equipment which is not normally running, but, which must start and run on demand.

Quantification of failure probabilities for these types of operational events differ, as follows:

The probability or frequency of failure for normally operating equipment is calculated as either:

- Interval unreliability, or, the expected number of times that the component will fail during a specified time interval {(MTTR+MTBF)/MTBF},
- Interval unavailability, or the fraction of time that the component is expected to be in a failed state during a specified time interval {MTTR/(MTTR + MTBF)}.

For standby equipment, the probability of failure is calculated as either:

- Unavailability, or the probability that the standby component will be in a failed state at any randomly selected future point in time (time of demand),
- Unreliability, or the probability that the equipment will fail to operate for a specified period of time (time of demand, or during its mission period).

Equipment is normally assumed to be non-repairable during its mission period, but may be restorable for future use.

Example:
In a 2-pump system, in which each pump capacity meets 100% of the system needs, the standby pump must start when the normally operating fails and must run until the normally operating pump is restored to full operability (mission time = operating pump MTTR)

The assumption is made that if the back-up pump fails during its mission, it is not repairable.

Calculations for the failure probability must consider each of the possible reasons that the equipment may fail to function on demand, e.g.

- Equipment is out of service for maintenance (unavailable — dismantled),
- Equipment is out of service for testing (unavailable — operational but not aligned to the system),
- Fails to start on demand because:
  (a) An undetected failure has occurred in the equipment since the last time it was used or tested (standby unreliability — failure in standby),
  (b) Equipment fails during start (unreliability — true demand failure),
  (c) Fails to start because the last time it was repaired or tested the maintenance or operating staff failed to restore it to full operable status (unavailable).
- Equipment starts on demand, but, fails to continue to operate for the time required (unreliability).

Examples of this type of equipment:

- Safety equipment which must actuate on demand,
- Air or motor valves which must open on demand.

The analyst:

- Examines the operating requirements for each component or basic event in the fault tree, event tree or reliability block diagram,
- Calculates the values for each appropriate term in the probability calculation,
- Inserts the summation of these values into the reliability model database.

Note:
Not all of these identified contributions to component failure probability may apply in a specific case, so the analyst must select only those which are appropriate.

Continuously operating equipment which is not directly involved in the process, but, must operate when needed to control an upset condition in the process. Monitoring and indicating instrumentation represent the most common examples of this type of equipment because they operate continuously, but, may not be actually used to control plant activities or initiate protective actions until a process upset occurs.

The probability of failure depends primarily upon the likelihood that:
- The equipment is out of service for maintenance (unavailable),
- An undetected failure has occurred (unavailable).

### *5.8.1.2. Definitions for hardware reliability/availability*

System types: – demand
– continuously operating

Demand: Two possible states, success or failure, i.e. "Component works or fails"

Observed failure rate, “l“= k/n
Observed success rate, S, = (n – k)/n

where:

n = number of demands
k = number of failures on demand
Note; S = 1 – l.

**Time dependancy of failures**

Suppose in the ith year of the life of a component there are $n_i$ demands and $k_i$ failures then,
l (I) = $k_i/n_i$
S(I) = $(n_i – k_i)/n_i$

If these are plotted for each year the trend in changing failure rate can be discerned and the rate of change calculated to determine if there are any ageing effects present. These effects are often thought to form the “bathtub” curve in which infant mortality is manifest as an above average failure rate early in life and ageing and wear out causes an above average failure rate late in life, although many equipment types exhibit time dependent failure rate curves which do not follow this classically assumed pattern.

A quick check of time dependency of failures over a given period of time can be made from a “time on test plot”. When the fraction of failures vs. fraction of time plot deviates from a straight $45^o$ indicates time dependency. If this line exhibits more than a single mode, i.e. changes direction, it often indicates the presence of multiple failure modes, with differing time dependencies.

**Continuously operating systems**

Operation is continuous except when down for repair:

$A(t) = 1/[1 + l\, t] =1 - U(t)$
Where:

"A" represents availability
"U" represents unavailability
$\lambda$ = failures per operating hour
J = repair hours per failure

Note:
A and U have no units, take on values between 0 and 1, and represent the average probability that a component will be in a successful (unsuccessful) operating state at any randomly selected point in time during a specified operating interval.

If the system has more than two operating states, i.e. can operate in a degraded mode of operation which is neither complete success nor complete failure, then the actual availability curve must be determined and integrated to find the average "equivalent" availability over the period. Frequently the SSC will have multiple discrete degraded states, so the availability curve is constructed as a set of discontinuous discrete areas which are added together to find the average equivalent.

**Sources of data**

The prime sources of data tend to be generic and are defined as:

- Failure rates — for initiating events and for continuously operating components and systems;
- Probabilities — for failure events which result because of, and after, the initial failure, e.g. startup of a standby/back-up pump, operator actions taken to limit the effects of the first failure.

Other databases are available, but, must be selected carefully to ensure that they are appropriate. Most component failure rates are strongly influenced by maintenance and quality assurance programme activities and practices (which in turn are driven by economic considerations). If a particular plant has a different or anomalous approach to maintenance, the data in an industry or international database may be inappropriate. If this is the case, plant specific data becomes very important!

#### *5.8.1.3. Collection of data*

Requirements for data collection and the levels of detail depend upon its ultimate use:

- To support systems reliability assessment,
- To support failure cause analysis.

For systems reliability assessment, the statistical pooling and treatment of data may be appropriate for failure rates and restoration times following a failure.

The data can be defined in terms of:

- A point estimate,
- A mean/median value with upper and lower bounds or other measures of data dispersion.

Typically, this data is used directly in the PSA and RAM models as:

- Best estimates, in which mean values are used,
- Bounding estimates, in which case the best/worst values are used.

If there is no appropriate component failure information, i.e. the component is not listed in a generic database or the service factor for the component is expected to be unusually harsh, then the data analyst must look for:

- Another database,
- Another plant with similar characteristics which maintains records of failure and equipment operating hours or demands,
- Other published reliability analyses for similar facilities or,
- Resort to estimates derived from knowledge of the expected conditions and hardware characteristics and expert knowledge of how these attributes may affect the expected SSC failure rate.

  In this case, data for components which appear should have similar characteristics becomes the starting point in the search for appropriate data, i.e. SSCs which have similar rotating masses, pressure forces, bearing types, and materials of construction.

- Elicit data from experienced plant maintainers, or vendors, who are considered to be subject matter experts in the characteristics of typical industrial and nuclear hardware.

For operating systems, (appropriate for O-RAP, but generally not useful during D-RAP), the elicitation or deduction of failure rates is focused on determination of the:

- Number of similar components which are installed,
- Number operating years experience the plant/components have,
- Number of failures there have been,
  (i) in the last year,
  (ii) in the last five years,
  (iii) since the plant was built.

Note:
When no failures have been experienced or recorded, assume that one failure has occurred, unless this gives an unreasonably large and unrealistic estimate, approximate failure rates.

For operating systems:

Component-operating hours= # Components * Hrs operation/Component-period per period

Failure rate = component failures/component-hours operation
per period per period

or, if there have been no recorded failures:

Failure rate = 1/component-hours operation
per period

For standby systems, required to operate on “demand”, the issues associated with calculation of failure rates involve determination of:

- The number of similar components which are installed,
- The frequency with which they are tested, i.e. once per shift/day/week/month,
- the experienced numbers of failures:
  - (i) in the previous year,
  - (ii) in the previous five years,
  - (iii) since the plant was built.

If the research indicates that "a failure has never been seen" — assume one failure.

The number of starts/actuations per period of time (year) and calculated failure rate:

# demands = # starts * # tests + # starts * startups
test year startup year
Failure rate = # failures per year (period)/# demands per year (Period)

For continuously operating systems whose failure does not result in an initiating event.

Operation of this type of system may be needed following an initiating event, as in the case of instrumentation which needed by a plant operator to guide his actions following a plant upset.

Instrument hourly failure rates are calculated in the same way as those for other continuously operating components, but, in addition it is necessary to know:

- The probability that if a failure occurs, it will be detected and corrected before it is actually needed to support plant operations.

  This will depend upon how often it is functionally tested during plant operations:
  - (i) Readings verified and logged so that an error or fault would be identified,
  - (ii) Whether there is an in-service testing program.

- The probability that at the time of demand or need the instruments are out of service for maintenance, which in turn, will depend upon whether component maintenance is normally performed during process operation.

The probability of the failure of instrumentation (unavailability)

P[instr.] = Failed hours/period hours
= Prob. instrument fails * time to detection
during operating period
= _Instr. failures * operating hours * average detection time_
operating hour test interval failure

Normally assume:
Avg. time to = Verification interval/2
detect failure

This same approach would be used for any operating system whose functionality is required during an accident scenario which follows the occurrence of an initiating event.

**Uncertainty**

An issue of concern to the user of failure rate information is often associated with the degree of confidence that should be placed in the data, or how much uncertainty there is embedded in the estimate.

There is always some variability in failure data, even when derived from the experience with very large populations: individual components have sufficient variability to cause a spread in the data.

This variability comes from:

- Variations in manufacturing and installation,
- Service factors — two similar components in different applications may experience different failure rates,
- Environmental conditions, i.e. heat, humidity, radiation, which can promote premature materials degradation or wear out.

Addressing the potential variability in reliability estimates requires use of failure rate distributions instead of point estimates so that areas of greatest importance and uncertainty can be re-examined:

- Focus on the areas of importance and greatest uncertainty,
- Propagate the uncertainty contributions through the models to provide an estimate of the uncertainty in the results which guide design and plant decision making processes.

#### *5.8.1.4. Failure data and reliability or availability models*

A reliability model is used to predict the frequency of occurrence for events which occur very infrequently. If an event occurs frequently, plant data will be available to describe both frequency and contributing causes and an "actuarial" approach can be used by the decision makers.

Very severe accidents occur very rarely so their frequencies may be completely unknown, or at best highly uncertain, so these are the types of events for which fault tree analysis is particularly useful for predictive purposes.

Many safety modifications involve the prevention of the "rare events" with "very large consequences" because accidents which happen frequently are just not tolerated by the general public, nor are they accepted by plant owners who suffer the costs. Normal plant design, operational practices and safety programmes generally prevent the occurrence of the accidents that can be easily anticipated.

### The rare event approximation

The existence and validity of the "rare event approximation" results from a simplification which is often taken during the development and quantification of reliability models which employ Boolean reduction algorithms in its processing.

When an "OR" gate has two inputs, events A and B, the probability of occurrence of the output is correctly calculated as shown below:

P[A+B] = P[A] + P[B] – P[A*B]

If the probabilities of events A and B are small (i.e. rare events), the term P[A*B] can be neglected. If the values used as data inputs are large (greater than 0.05) the error from the approximation algorithm may start to become large.

This means that to maintain the validity of calculations performed with techniques which use the rare event approximation, ALL basic event magnitudes should have values below 0.05.

### Maintainability data

Though there is some uncertainty in the data for SSC failure rates, there is often an even greater degree of uncertainty in maintainability data or average SSC downtime. There are a number of reasons for this, primarily because the time taken to repair an SSC is very much affected by the maintenance environment and conditions surrounding the repair process. In addition, much of the focus on data collection has been driven by the need to quantify PSAs, and since safety systems are generally considered to be unrepairable, there is much less need for repair data than there is a need for failure rate data, and there has been much less focus on its collection.

### Variability in maintainability data

Some of the reasons for a great deal of the variability in plant-to-plant maintainability data, include:

- Differences in the availability of staff to initiate the repair at the time that failure is detected, i.e. whether or not the plant uses round-the-clock maintenance or limits the maintenance staff to day work, unless “called in” for important SSC failures,
- Whether the plant defers maintenance to prevent call-ins and to control overtime, for all but the most important SSCs,
- The skill, experience and training of the maintainers,
- Whether the SSC design is inherently maintainable,
- The extent to which designers considered SSC maintainability during plant design and layout.

In many cases, the existence of appropriate data in a generic database is very limited and for new designs, a great deal of the repair data to be used in a RAM equivalent availability model must be derived from an expert knowledge of the design and from expert opinion in which available maintainability or down time information taken from documented data sources is modified to provide a plant specific equivalent.

### 5.8.2. Plant database — human actions

This section of the guidebook introduces the Issues of the reliability of the man-machine interface. The performance of hardware is intimately related to the extent and manner that the human interacts with that hardware. This interaction places the human in two distinct roles:

- As an adjunct to the hardware, in which the human is an extension of the hardware and acts as a controller:
  - (i) typified by that of a process operations manager, process control room operator or an individual machine operator,
  - (ii) actions limited to modulating controls or turning equipment on and off.
- As a vital auxiliary or support system for the hardware in which the human dictates the quality of its performance:
  - (i) typified by the maintainer, the QC inspector, or the equipment tester,
  - (ii) "quality" of hardware performance is measured by two parameters, the expected time between hardware failures (MTBF) and the expected time to restore following failure (MTTR).

Clearly to calculate the reliability for a system in which the human plays a controlling role, the human action must be included in the analysis, and appropriate measures of human performance established. Since the human in this role is working in a mode which is analogous to an element of hardware, and only two parameters are necessary to describe hardware performance, there must be comparable performance measure attributable to human failures:

- Failure rate or is equivalent "human error probability" (HEP),
- Conditional probability that successful restoration will occur within a defined period of time, or its human equivalent, the probability of recovery from an error, in a defined time under a defined set of conditions.

These similarities in the nature of human and hardware performance, imply that if human performance data can be specified, human (un)reliability can be quantified in a manner which is analogous to that routinely used for hardware.

There are several sets of data which can be used to quantify human reliability, depending upon the nature of the activity, each of which employs a similar approach, namely the definition of a technique which uses event specific conditions to modify a standard error rate defined under specified conditions. This is made necessary because the probability of human error is dependent upon the events which went on beforehand, i.e. all HEPs are conditional probabilities. i.e. conditional upon preceding events.

This concern for conditionality also applies to hardware failure probabilities but there is one important difference, the degree of variability in the conditioning events is far less. This means that the preconditioning of hardware is far more predictable, so the variability is lower.

Generally there are three approaches used in the calculation of human error probabilities:

- Collect actuarial data for various known human activities and modify them for the actual specific conditions (influence from experiments).

- Use expert judgement to assess the importance of conditions and their impact on human error rates.
- Identify classes of human activities and determine whether there is a way to treat them in blanket fashion.

This latter approach becomes the key to understanding a broad spectrum of human activities in a pragmatic fashion. This same information also implies that quantification of human reliability will also require the development of a model which relates each influence on human reliability, often called "performance shaping factors", to the corresponding human error probability and that selection of a single data point from a database will likely never suffice.

#### *5.8.2.1. General methods used to model human reliability*

General methods used the modeling of human reliability include:

- Reliability block diagram analysis,
- Fault tree analysis,
- Event tree analysis.

With each of these methods, the human action is modeled explicitly as either a contributor to failure (error) or a mitigating factor, in which the human action reduces component unavailability (recovery).

Examples of human actions which contribute to unavailability include:

- Inadvertent disabling of the component following a test or maintenance activity,
- Initiation of a system transient,
- Failure to follow procedures to terminate an event in progress,
- Perform activities make a bad situation worse.

Examples of positive human influences which increase system reliability include:

- Use of procedures to recover non-functional hardware by finding new success paths or changing process conditions to facilitate hardware operation, e.g. depressurization of RCS to allow low pressure ECCS to function, following failure of the High Pressure ECCS system,
- Improvise and restore or repair previously failed equipment.

Our task is to understand how these human actions can be incorporated into our models, and how they can be quantified. It is immediately apparent that human actions fall into two categories:

- Errors which result in contributions to component unavailability,
- Errors in performing actions which actuate hardware systems.

In the former case the action is implicit to component unavailability, whereas in the latter case the human action is explicitly modeled by the reliability model logic.

Examples:

“Failure to restore" is assessed as a contributor to unavailability

$U_{FRFM}$ = _maint. tasks_ * restoration failures * time
time task failure

Similarly for test restoration errors:

$U_{FRFT}$ = tests * restoration failures * time
time test failure

Failure of the human to actuate hardware is quite different, because in this case the human fails "on demand" and is viewed in a manner much the same as for that of hardware. It is interesting to note the similarities in the conditions which initiate demand failures for humans and hardware.

A component fails to operate on demand at time, t, if it:

(i) is unavailable at time, (t – delta t) because it is:
- unrestored following test or maintenance,
- unavailable due to test, or,
- unavailable due to maintenance,

(ii) fails on demand at time, t, because it:
- failed during standby operation in an undetectable mode,
- fails during the demand, or,
- fails during the ensuing period of the mission, (t to t + mission length).

The human has analogous failure modes:

(a) Unavailability at time, (t – delta t) because he is not physically present, present but is totally preoccupied, has a low state of awareness (asleep, analogous to a “standby” failure) or reassigned to other tasks (analogous to a failure to restore);

(b) The human fails on demand at time, t, because the actuation signal received, the action commences and then fails.

This can result from mis-interpretation of the demand, (diagnostic error), an incredulity response in which no action is performed (fear), or, correct diagnosis which is followed by an error in implementation.

From the preceding, a case can be made for looking at human behavior in much the same way as hardware behavior. The analogy may not be rigorous, but it provides some useful insights into how a method (or methods) can be used to expeditiously calculate numerical estimates of the probability for success of failure for a given human action under a specified set of conditions.

#### *5.8.2.2. Human behavior and decision making*

There is evidence to support the thesis that there are three different regimes of human behavior, which in increasing levels of abstraction, are:

- Skill based behavior, in which the action is a short term, frequently rehearsed action which becomes a reflex action, e.g. pressing the reactor trip button when needed, stepping on the brake pedal in a car to stop for a red light;
- Rule based behavior, reflects the mental behavior which a human exhibits when following proceduralized rules, e.g. following a plant procedure to achieve a specific goal, following a “right turn on red” rule when driving a car;
- Knowledge based behavior, is non proceduralized behavior, in which the human establishes a “goal state”, determines his current state relative to the goal and formulates and implements a strategy to achieve it, e.g. when the plant operators at TMI had an undiagnosed PORV leak they established a goal state involving protection from pressurized thermal shock, instead of core protection, and implemented a strategy (securing the ECCS system) to achieve it. They were beyond the range of the then-current emergency operating procedures and operating “cognitively”, i.e. thinking and acting, not following a set of rules.

**The human as a control system**

In the nuclear power plant, the human role is one of systems controller in which he monitors the process, collects information and processes it to infer a “process state” and then compares this process state with a desired or "goal state".

Deviations between the actual and desired process states results in the development and implementation of a strategy which will move the process towards achievement of the desired state. Several discrete steps or activities must be successfully concluded before the human can operate effectively within this control loop. The human must:

- Detect, receive and discriminate needed information,
- Use the received information to infer the state of the process,
- Compare the inferred process state with the goal state to assess the need for change,
- Formulate a strategy to move the process towards its goal state,
- Carry out the strategy correctly to achieve the desired system goal state.

There are numerous opportunities for the human to make errors. During sensing, information processing and during the mechanical implementation process, and the likelihood of error is influenced by factors within, and outside, the human:

- Environment — stress,
- Information display,
- Innate capabilities and experience.

Consideration must be given to all of these factors, during prediction of the HEPs and in their prevention during the design process.

### *5.8.2.3. Hardware vs. human performance*

For hardware there is a wealth of empirical evidence for statistical estimates of failures, whereas for human performance there is a very poor database which gives good estimates of human performance. This is because individual hardware component types achieve individual (specialized) functions which limit the variability in performance:

- Hardware applications are predicated on expected service conditions,
- Definition of success and failure is fairly easily described.

Human failures are different because when a human fails it is not always obvious and errors may be hidden. In addition, human variability is large because a single human may fulfill many different roles and he may be ill-adapted to perform the task in hand. Not all humans have the same capabilities (inherent) and human performance is affected by "conditions".

### *5.8.2.4. Human reliability assessment methods*

**Method (1) — Technique for Human error rate prediction (THERP)**

Reference “Handbook of Human Reliability analysis with Emphasis on Nuclear Power Plant Applications”, Sandia National Laboratories, NUREG/CR-1278.

This comprehensive handbook provides an analytical database and procedures and methods for adapting the information to plant specific conditions so that an human reliability analysts can estimate the probabilities of error in performing specific human actions which are important to the reliability, safety or economy of a nuclear power plant. The bibliography in Annex 1 identifies additional sources of information which further describe THERP and the advancements made since publication of the handbook, particularly in streamlining the process using screening criteria and simplifying, yet conservative assumptions.

The THERP methodology is intended to support conventional systems reliability analyses in which human events, important to system reliability, are identified by the systems analysts. Human reliability analysts examine these events and determine which human errors are to be defined and analyzed, then taking data drawn from the handbook, expert judgement, or any other available sources, estimate the important error probabilities.

Limitations in the methods are well defined in the handbook, but, include uncertainty in the data, uncertainty in understanding human behavior and uncertainty in the model and how the human interacts with the hardware. The translation of nominal human error probabilities (HEPs) into the specific values used in the analysis (performance shaping factors) is founded on the following basis; unless stated otherwise the HEPs provided in the THERP database are based on the following standard conditions:

- Plant is in a normal operating state and the operator stress is optimal,
- No protective clothing is required for the performance of the activity of interest,
- An average level of administrative control is in effect,
- The tasks are performed by qualified personnel and are experienced to the degree that they have been in the position for six months,
- The operator's environment is not adverse.

The product from the analysis is a set of estimated plant- and situation- specific human error probabilities. Since within D-RAP, the plant and procedures do not actually exist, assumptions must be made. The important effect must come from the fact that after the procedural requirements have been recognized, recommendations for their content can be made on the basis of the HRA analysis, i.e. they are optimized.

Implementation of THERP takes place in several phases:

- Plant and target action familiarization, i.e. assess the expected environment in which the human is going to perform the activity of interest, allow the analyst to become familiar with the operations relevant characteristics of the facility and to identify facility characteristics (layout) and administrative control systems which affect the **generic** human performance (no evaluation of individuals at this time);
- Qualitative assessment, i.e. review information from systems analysts for a given scenario or sequence of events and obtain clear definition of the human action which directly affect the system-critical issues and use this information to assess these actions within the context of their actual performance and determine whether any important influences on behavior in these system critical activities may have been overlooked;
- Quantitative assessment, i.e. modification of the nominal HEPs is based on the information found to this point and used as the basis for the remainder of the quantification process. As defined in the handbook, “A human action (or its absence) constitutes an error only if it has the potential for reducing the probability of some desired system event or condition". The tasks involved in the quantification of the HEPs include completion of:

  (i) A detailed task analysis in which the target human actions are broken down into individual units of behavior and specific potential errors of omission and commission are identified for each unit of behavior shown in the task analysis,
  (ii) Development of a human reliability model from the task analysis in which error events are placed in chronological order and assigned with the nominal probabilities adapted from the handbook,
  (iii) Estimating the effects of performance Shaping factors (Puffs) i.e. modification of each nominal HEP to reflect the actual performance shaping factors appropriate to the situation and to compensate for any dependencies between tasks or individual operators participating in the performance of the target action,
  (iv) Determination of Success and failure probabilities and their propagation through the human reliability assessment (HRA) model to find the overall probability of success or failure for the activity,
  (v) Assessment of potential recovery factors for errors which are important and modification of the model to find the predicted HEP for the target action under the expected conditions.

THERP is particularly useful for analysis of human actions which are sequential, rule based and performed by individuals, but can be very difficult to use when activities are performed by a crew of people in a dynamic fashion. The approach discussed above does not explicitly address DDD (detection, diagnosis and decision) errors, but, they are part of THERP.

**General time-reliability correlation and THERP**

Within THERP, there is a diagnostic time-reliability correlation which is able to serve as a screening precursor to a detailed THERP analysis by allowing for the inclusion of the possibility that detection, diagnosis and decision errors will dominate the failure probability.

An alternative model has been proposed to overcome some of these difficulties, namely the human cognitive response model developed by EPRI.

This model has encountered some difficulties when compared with results taken from simulator tests, but, has value as a means for predicting non-response probabilities for operating crew activities. The difficulties encountered with the HCR model may originate with the premise that there is a time reliability correlation for human actions carried out within each regime of human behavior, i.e. skill, rule and knowledge based, but target actions often represent a mélange of activities which embrace more than one regime.

**Method (2) — the human cognitive response (HCR) model**

The HCR model, developed by EPRI, attempts to address this situation by using data collected on the response of different crews to simulated events. Observation of operators during simulated severe accidents indicates that:

- The time required for an average crew to achieve a successful outcome depends upon the number and complexity of the required actions,
- For different situations there are significantly different ways in which the crews can be successful,
- The cumulative probability of significant non-successful actions decreases as a function of time.

The HCR model provides one method for quantifying the reliability of control room crew actions by defining a mathematical model of the non-response probability which has the following characteristics. The HCR model:

- Is reviewable and repeatable,
- Compatible with current reliability assessment techniques,
- Results in quantification of crew success probability as a function of time,
- Considers different types of cognitive processing (skill, rule, knowledge),
- Identifies the relationship between the model and influencing factors on non-success probability:
  - (a) Plant design features,
  - (b) Operator training and experience,
  - (c ) Stress,
  - (d) Misdiagnosis and recovery,
  - (e) Time available for action,
- Can provide results which are comparable with existing data from plant experience, simulators or expert judgement, for specific well defined target actions,
- Is simple to use,
- Provides or generates the necessary insights and understanding about the potential for humans to cope with various situations.

The HCR model was developed from a recognition of the importance of various influences on human behavior, and specific contributions from:

- Time reliability correlation,
- Empirical technique to estimate operators errors (TESEO),
- Rasmussen mental schematic,
- Simulator data.

**HCR time reliability correlation**

A normalized time-reliability curve, whose shape is determined by the associated dominant human cognitive processing regime, is at the core of the model. The normalized time is the actual time available to perform a specific task, divided by the median times taken by crews to perform this task.

Currently, this median time is derived from simulator measurements, task analyses and expert judgement.

The basic normalized curves are developed from simulator data, and the dominant cognitive processing can be determined from a logic tree and the effects of operationally induced stress, control room equipment layout, etc. are accounted for by the modification of the median time.

Although the HCR model is called a model it is really a mathematical correlation and the shape of the curves can be approximated with a three-parameter Weibull distribution.

**Use of the HCR model**

The possible decision activities which the crew faces during a given event is first identified and the HCR model is used to quantify the non response part of the tree. Three non-success outcomes are possible:

- Non-response,
- Misdiagnosis,
- Selection of a non-viable option.

The fourth outcome, success, can then be further analyzed with THERP.
Consideration of the three options allows explicit consideration of the treatment of no response, faulty response, and correct response. Quantification of the HCR non-response model is performed by following the steps listed below:

- Identification of the key factors associated with the situation to be analyzed, i.e. the type of cognitive processing,
- Estimation of the median response time for the crews to perform the required tasks, obtained from simulator data, operator interviews, engineering judgement,
- Modification of the median response time to account for the performance shaping factors, e.g.. stress, information interface and operator experience,
- Estimation of the available system time window from simulations (T-H analysis), similitude with previous response analyses and expert judgement,
- Derivation of the non-response probabilities from the HCR curves for the specific situation being modeled.

#### *5.8.2.5. Applications for HRA in design*

The two basic approaches described above represent two functionally different ways of predicting human reliabilities for specific target actions under specific conditions, typically defined from the characteristics of specific accident scenarios or plant upset and transient events. There are other methods which can be used, but, ultimately whichever one is selected by the D-RAP team, its use will be somewhat similar. More than one method may be used in the course of a comprehensive evaluation because some methods are more effective in predicting the outcome for specific types of events, and some are more effective than others when used for screening.

Many events are explicitly included in the D-RAP PSA and RAM models, and to perform a detailed analysis for each one would be very resource intensive. To control the scope of the HRA, "screening analyses" are used to identify approximate, yet conservative values, for individual HEPs, and the models re-solved to identify those which are important, i.e. have an important effect on the calculated risk. A refined analysis using one or more of the latest HRA techniques will be performed to better define the HEPs for important target human actions, and the screening values will remain for those of lesser importance. The results from the analysis will be a rank-ordered list of human actions, comparable to the list developed for SSCs, and used to guide the design team in their development of the man-machine interface.

#### *5.8.2.6. Human factors*

There is a difference between human factors and human reliability, but, both are important to the D-RAP process. Human factors engineering is the term generally given to the ergonomic design process for development of the plant wide man-machine interface. Human factors engineering ensures that the plant hardware and human environment are compatible and focuses on the physical aspects of the interface between them. A few examples of the very many ergonomic considerations which must be part of the design process for the man-machine interface include specification of:

- Height, size, color and type of indicators and control panels and the layout of CRTs and computer indication, alarm and advisory information,
- Mimic buses to improve the flow of information from the process to the process operator,
- Tactile feedback on controls and switches,
- Avoidance of conditions which violate populational stereotypes, e.g. switches and indicators which turn left to right, instead of right to left, mirror image control rooms in multiple units, or warning light colors which oppose the red/green convention,
- Hierarchy of alarms and concern for operator information overload,
- Operability, i.e. ensuring that the process time constants are consistent with human capabilities, wherever human intervention and control is required,
- Unambiguous and clear labeling of all plant components and the use of standardized color coding to ease in the rapid identification of all classes of SSCs, their expected operating states and their system affiliations.

An effective and efficient ergonomic interface is essential to the reliability and availability of the plant because its effectiveness affects every aspect of the man-process interaction, and establishes the basis for "good" or "poor" human reliability for every target human action. The ergonomic interface provides a precondition which influences the error probability for every human action implemented during both routine, normal and off-normal plant states or conditions. Generally, the design team implements the ergonomic interface on a plant-wide basis through set of deterministic criteria which ensure implementation of the "best possible" human factors practices.

The rank-ordered list of target human actions can be used to focus the development of the ergonomic interface, or at least confirm that it is optimal under a small set of plant conditions. However, its more important role is in the determination of other aspects of the man-machine interface which play a strong role in determining the reliability of the human. In this case, the design team looks at the human interface from a different perspective, as briefly described below.

The D-RAP human design team looks at the conditions surrounding the performance of each important human activity identified on the rank-ordered list and uses the results from individual human reliability analyses to confirm the viability and acceptability of specific aspects of the design which are important to reliability. Some of the more important goals for this analytically guided design review of the man-machine interface may include confirmation that:

- The information presented to the operator is sufficient to guide his decision making process effectively, i.e. the information presented is sufficient to detect, diagnose and correct any off-normal conditions within the time available,
- There are no obvious ergonomic deficiencies which will have an material negative impact on the non-response probability for the target action,
- The issues which are important to the completion of the task are defined so that when procedural guidance is prepared for the operator, it contains all of the necessary relevant and helpful information,
- The plant simulator is capable of reproducing the plant conditions which mimic and surround each important target human action,
- Automatic protective actions implemented by hardware control and instrumentation systems are sufficiently reliable, and that over-reliance on the operator as an operations system manager is not negatively affecting plant risk.

The D-RAP design team will use the rank-ordered list of target human actions in a way which is directly analogous to the way that they can be expected to use the rank-ordered list of SSCs which are important to both safety and economy.

## 5.9. RA PROGRAMME DOCUMENTATION

### 5.9.1. Introduction

The documentation for the D-RAP should be of a level of specificity and detail to completely define the programme and should generally have the following functional characteristics:

#### *5.9.1.1. Deterministic requirements*

To ensure that the programme does not inadvertently lead to the violation of prescribed deterministic criteria, or other commitments made or required of the plant owner, it is important that these requirements are clearly and unambiguously defined before the design process is initiated. Though identified as a requirement of the D-RAP documentation, they may be described in the preliminary safety analysis report and included in the D-RAP by reference. The important issue is that they be fully recognized, because they either remain as constraints upon the D-RAP optimization process, or become the targets for change if they are found to be inappropriate or pose too severe a financial burden with little, or no, positive economic benefit.

In large measure these criteria and requirements will embrace the design basis scope described by the requirements detailed in Figure 2-3, namely:

- Regulatory requirements,
- Probabilistic safety goals and performance criteria,
- Requirements from the Utility Requirements Document (Reference: EPRI Advanced Light Water Reactor Utility Requirements Document (3/90)) or an equivalent adopted by other IAEA Member States,
- Applicable codes and standards,
- Specific commitments made by the owner operator to any cognizant regulatory authority.

#### *5.9.1.2. Implementing procedures*

Each of the RAP functional elements should have its own implementing procedures to ensure that the programme requirements are applied consistently. Consistency is essential because it is only after consistency is achieved that continuous programmatic improvement can be effected throughout the remaining life of the design.

The D-RAP must be seen as a living programme which can be enhanced to improve its effectiveness whenever, and wherever, the need for change is recognized.

### 5.9.2. Quality standards for RAM and PSA models

Quantitative support for the RA programme, and ultimately the success of D-RAP will depend upon the fidelity, quality and traceability of the models which are used to guide the management processes which assure optimum plant safety, reliability and economy.

Without a high level of assurance of the quality of each of these facets of the RAM and PSA models, their use in the definition, or redefinition of the plant design basis will be limited. In brief, this means that the plant RAM and PSA models must have:

- Analytical or experimental evidence (safety analyses) to confirm functional and transient plant behavior which can be expected to follow the complete set of initiating events or generating system component failures included in the RAM and PSA model logic,
- Documented and traceable success criteria for all safety and generation systems,
- Clear documentation of the inter-linking dependency network between all systems and components,
- Representative failure and repair data and comprehensive technical procedures which assure its optimum value towards the prediction of failure probabilities and frequencies,
- Clearly defined system behavior and assumptions made about the various modes of system operation,

- Clear definition of the role of the human in the management of the safety and generating systems and the bases for assessing the reliability of the human when fulfilling this role,
- A defined file structure and access system which will provide adequate QA for the plant models, and provide and maintain configuration control for the models,
- Computer codes which meet recognized verification and validation standards,
- A procedure which defines the objectives and protocols used to review the RAM and PSA models and confirm that they are adequate to support D-RAP,
- An effective administrative procedure to guide the upgrading of the RAM and PSA models so that they parallel design evolution and maintain their fidelity to the "as built" plant.

Generally the PSA and RAM models could be expected to satisfy each of the functional dictates of the plant quality assurance programme.

### 5.9.3. Quality standards for documentation of PSA and RAM results

The numerical results provided by the RAM, PSA and associated economic or other deterministic models will be used to provide information which supports the development of the final plant design. As a consequence, there should be a predefined set of guidelines or functional procedures which indicate how these results are to be used. These procedures will ensure that:

- Results are not used out of context,
- All decisions are made with a full understanding of the implicit, and explicit, limits and assumptions introduced by the modeling process,
- Sources of potential, or actual, uncertainties are recognized and that there are procedures available to guide the decision maker whenever the levels of uncertainty are unacceptably high for a specific application, i.e. provide guidance in the ways to reduce uncertainty when absolutely needed to make a decision.

These application procedures should also provide guidance on how the results should be used and the conditions under which a streamlined approach may be both desirable and effective.

## 5.10. MAXIMIZING SSC MAINTAINABILITY

In addition to having a concern for the complexity or frequency of maintenance which in turn may lead to a higher than necessary maintenance error rate which has an impact on component reliability, there is also a concern for SSC maintainability. This is the case when the SSC ranking and characterization process indicates that availability or average down time is a dominant contributor to its importance. In this case the focus shifts from examination of the impact that maintenance has reliability, to an assessment of how to minimize the average down time, or restoration and repair time which is associated with each preventive and corrective maintenance action. The potential contributors to SSC down time are depicted in the simplified goal tree shown in Figure 5-9.

### 5.10.1. Minimizing mean down time (MDT) from preventive maintenance requirements

The designer is generally unable to influence the requirements for some routine preventive maintenance activities because they are established by the equipment manufacturer, and are presumably based upon his experience with its basic design characteristics and operational experience with similar equipment. The important thing is that the SSC procurement specifications request the preventive maintenance schedule so that the costs from PM down time can be calculated and compared for each offering, and an evaluation of their relative magnitudes used to influence the selection process, to the point that the benefits from reduced down time are commensurate with the benefits to safety and economy.

Note:
It could well be that, later in the design phase or early in the operational phase, an effective reliability centered maintenance (RCM) programme may justify a reduction in frequency for the required maintenance or a shift from periodic to condition directed maintenance. At the time that the procurement process is initiated it is unlikely that the RCM programme will have been developed, however, if it has been, the insights it brings should be factored into the SSC specification and evaluation process.

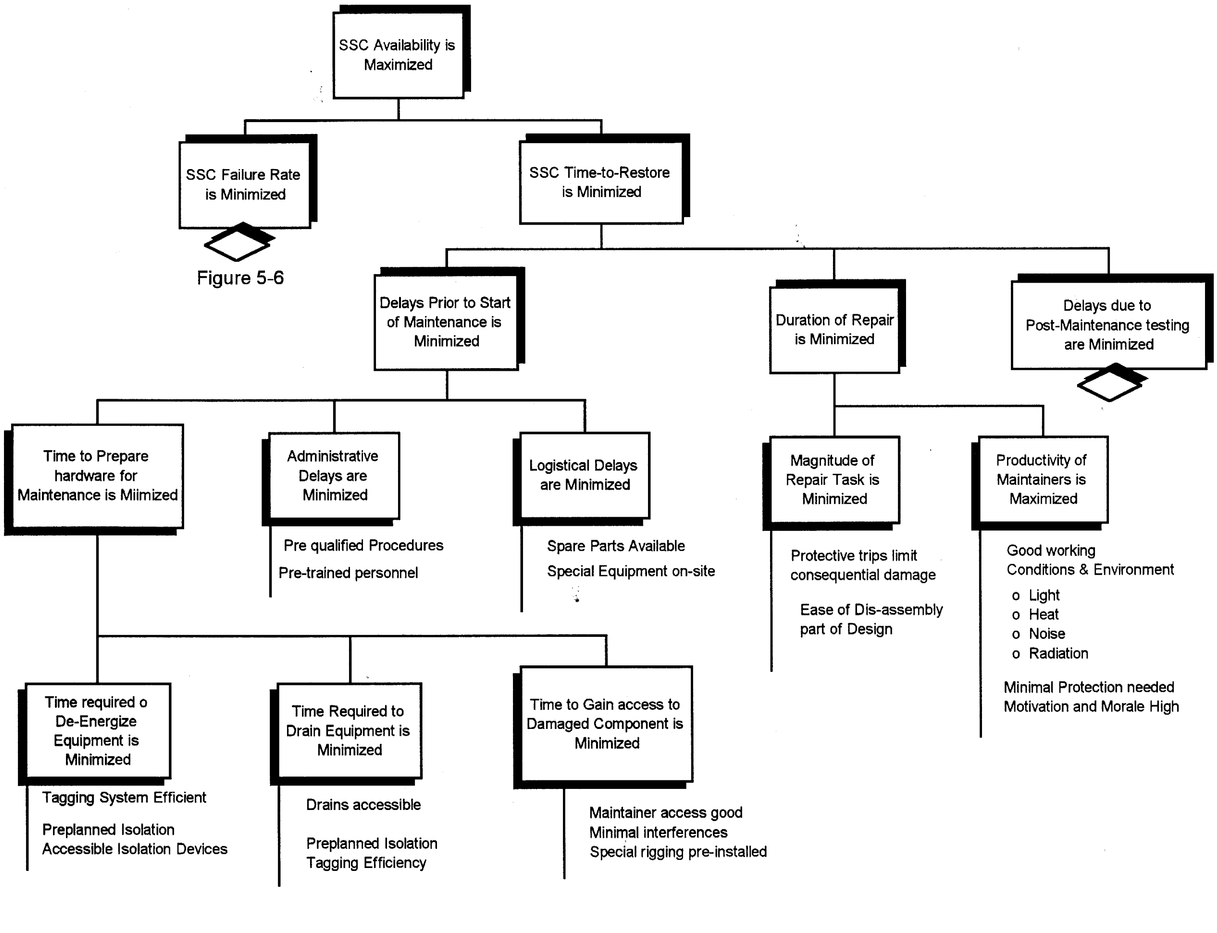

SSC Availability is Maximized
SSC Failure Rate is Minimized
Figure 5-6
SSC Time-to-Restore is Minimized
Delays Prior to Start of Maintenance is Minimized
Duration of Repair is Minimized
Delays due to Post-Maintenance testing are Minimized
Time to Prepare hardware for Maintenance is Miimized
Administrative Delays are Minimized
Pre qualified Procedures
Pre-trained personnel
Logistical Delays are Minimized
Spare Parts Available
Special Equipment on-site
Magnitude of Repair Task is Minimized
Protective trips limit consequential damage
Ease of Dis-assembly part of Design
Productivity of Maintainers is Maximized
Good working Conditions & Environment
o Light
o Heat
o Noise
o Radiation
Minimal Protection needed
Motivation and Morale High
Time required o De-Energize Equipment is Minimized
Tagging System Efficient
Preplanned Isolation
Accessible Isolation Devices
Time Required to Drain Equipment is Minimized
Drains accessible
Preplanned Isolation
Tagging Efficiency
Time to Gain access to Damaged Component is Minimized
Maintainer access good
Minimal interferences
Special rigging pre-installed

*FIG. 5-9. Contributors to SSC unavailability — down time.*

### 5.10.2. Minimizing mean down time (MDT) from corrective maintenance activities

Maintainability review to assess the impact of design decisions on the mean down time needed to perform corrective maintenance for important SSCs is very important to D-RAP because the design team has a great deal of influence over its magnitude. Down time contributions from corrective maintenance have several generic origins, each of which is described in detail below.

Contributions to average down time can be broken down into the following general categories, which in turn are expanded to identify each individual cause which can potentially contribute to lost service time. Though all of the discrete contributors to down time are described for the sake of completeness, not all can be remedied by the D-RAP team. Some will be resolved during operation. However, where important contributions to SSC MDT are recognized, the D-RAP team should identify them so that they can be incorporated later in the RAP process.

The broad general sources of time expended during corrective maintenance, and their individual contributing mechanisms are as follows:

- Time lost from the time that the failure occurs to the time that it is detected and remedial actions are initiated by the plant staff. This contribution is a particularly important contributor to the probability that a standby safety system SSC will not start on demand, and can be caused by inadequate monitoring (instruments or periodic inspection) which is able to provide evidence of functionality and operability and annunciate it to the plant operating staff,
- Time lost from the time that the failure is detected until corrective actions are initiated on the SSC:
  - (a) unavailability of on-site repair staff (primarily under the purview of O-RAP),
  - (b) time required to establish the work scope boundary and tag-out, de-energize and/or drain the system components within the tag-out boundary,
  - (c ) time required to remove interferences to provide necessary access to the work,
  - (d) time needed to build scaffolds to provide ready access to work area,
  - (e) time required to remove thermal insulation and provide access to SSC,
  - (f) time required to install shielding to allow worker access to high radiation area,
  - (g) time required to obtain needed special tools and repair equipment or to establish rigging needed during the disassembly or removal process.
- Time required to perform the repair, following completion of all preparatory activities which is the result of:
  - (a) Time lost because of the difficulty or complexity of the required task, or delays from required set-ups, tooling and machining activities which cannot be performed on-site,
  - (b) Time lost because the SSC protective trip and fault isolation systems fail to prevent consequential damage and cause an unnecessary increase in the magnitude of the needed repair activity,
  - (c) Time lost during performance of the required corrective actions from worker inefficiency which is the result of:
    - (i) Inadequate lay-down area,
    - (ii) Inadequate tools,
    - (iii) Poor failure diagnostics which lead to poor job planning,
    - (iv) Shortage of spare parts,
    - (v) Shortage of trained and/or experienced maintainers,
    - (vi) Poor environmental conditions (light, heat, ventilation),
    - (vii) Need for excessive personal protective equipment (air-breathing apparatus, plastic anti-contamination suits, etc.).
- Time lost from the time that repairs are complete and the component is restored to full operational status:
  - (a) Time lost when refilling or re-energizing equipment,
  - (b) Time lost when setting up, and performing, post maintenance functional testing.

When the designer is developing the specifications for an SSC whose importance is a result of its unavailability or high average mean down time, each of the issues listed above must be considered. The specifications and associated request for proposal (RFP) must both define the maintainability targets for the SSC and elicit the information needed to evaluate each offering within this context.

## 5.11. OPTIMIZATION OF PLANT TECHNICAL SPECIFICATIONS

plant technical specifications are a set of licensing specifications which impose operational constraints and requirements on the plant in order to meet several important objectives, one of which is providing assurance that the plant never strays beyond the operational boundaries assumed during performance of the plant safety analysis. These technical specification requirements provide assurance that the plant will always operate with a minimum number of operable success paths which are capable of maintaining each critical core and plant protection function following the occurrence of each predefined design basis event under its assumed boundary conditions.

For the purposes of both maximizing plant safety system reliability and facilitating maintenance and testing activities, these functional success paths are designed to be both redundant and diverse, the latter so that the effects of common cause failures are minimized. The plant technical specifications, or their equivalent in member states other than the USA impose restrictions upon configuration of these success paths and effectively limit the extent to which temporary reductions in redundancy and diversity can be made during in operating mode.

Generally, these restrictions are in the form of allowed outage times (AOTs) for specific trains, however they also include restrictions upon the number and nature of the safety system trains which can be rendered unavailable at any specific time. These restrictions challenge the plant's ability to perform on-line maintenance and at times lead to the need for an extraordinary exemption from the requirements, or, in the event that one cannot be approved in a timely manner, for a plant shutdown.

Current technical specifications were generally defined before the advent of a PSA for every plant, and before the quantitative insights gained from their wide-spread performance were available to the regulatory agencies. This need not necessarily be the case for ALWRs, since performance of a risk and reliability assessment will be part of the design decision-making process. As a result, it should be possible to examine the predicted plant risk profile and make intelligent decisions about allowable plant configurations which are not nearly so restrictive as those imposed on the current generation of plants. They should err to the conservative side, but, should also provide pragmatic opportunities for on-line plant maintenance.

In the future, the plant's need to perform as much on-line maintenance as possible will be pressured by a need to minimize the amount of work required during planned outages. When future goals for planned outage rates are lowered to a target range of 5% (equivalent to 18 days per year), the need to perform preventive maintenance and surveillance testing activities during power operation, instead of during shutdown, will increase. To achieve this, changes in the allowable outages for safety systems and safety system trains must occur.

The following describes a general approach which can be used within D-RAP to provide the technical basis for such a transition, although, whether it can be adopted by future plant licensees will depend very much upon the willingness of cognizant regulatory authorities to approve such changes. It is important that this regulatory issue be resolved early in the plant licensing process because in the PSA, the probabilistic contributions from unavailability due to test and maintenance will depend upon the freedom offered by the plant technical specifications. The comprehensive use of PSA to optimize safety system design will depend upon prior resolution of this issue.

### 5.11.1. Optimization of technical specifications — configuration

The base design can be used to define a set of technical specifications after its conversion in the following manner:

Remove all contributions from unavailability which are attributable to test and maintenance activities and calculate a baseline core damage frequency, and if desired, the source term release frequencies, for each power state of interest.

Typically, the power states of interest will be those which represent the plant operating modes within which technical specification optimization is desired.

- Initiate a predefined sensitivity analysis in which individual sub-systems or safety system trains are removed from service (set to a “failed state” in the PSA models) and develop a correlation between risk (using the surrogate measure of choice) and configuration:
  (i) Loss of one, or more than one, trains in frontline systems which serve the same plant critical function,
  (ii) Loss of one, two, or more than two trains in frontline systems which serve different plant critical functions,
  (iii) Loss of one, two, or more than two support system trains (AC, DC, cooling water, etc.).
- Use predefined acceptability criteria for identify those configurations which would not be allowable, and those which could be tolerated for a specified period of time. The magnitude of the conditional increase in risk (CDF) would be the determinant of the time which would be tolerated, and:
  (a) Identify the configurations which must be prohibited,
  (b) Identify the configurations which can be allowed to occur for some specified periods of time, e.g. less than 2 hours, up to 8, 24, 72, 144 or 312 hours.

Note:
The acceptable thresholds for a predicted conditional increase in instantaneous risk (CDF) over a specified period of time must be developed and accepted by both the owner and the cognizant regulatory authorities, before they can be used.

The results of the foregoing will be a set of allowable plant configurations, and an associated set of times which limit the length of stay that the plant may have in any specific configuration. The relationships between the predicted conditional change in CDF and the duration and safety significance of the configuration, must be predefined. Although the following example of a possible numerical approach may be arbitrary, it may also be useful to put the concept in context.

For example, assume that:

- After contributions from unavailability due to test and maintenance have been removed from the baseline level 1 PSA, the current CDF is 1E-5/a (average CDF of 1E-9/h),
- If a specific configuration were to be implemented once a month and the average annual CDF does not increase by more than 100% (to 2E-5/a), the risk is acceptable.

This implies that, to be acceptable, the increase in conditional change in hourly CDF which follows the plant's transition into a specific configuration, must be no greater than:

- 4E-5/hour for 2 hour duration (hourly CDF increase × 400),
- 1E-7/hour for 8 hour duration (hourly CDF increase × 100),
- 3E-8/hour for 24 hour duration (hourly CDF increase × 30),
- 1E-8/hour for 72 hour duration (hourly CDF increase × 10),
- 6E-9/hour for 144 hour duration (hourly CDF increase × 6),
- 3E-9/hour for 288 hour duration (hourly CDF increase × 3).

Though the above numerical values are somewhat arbitrary, they show how it may be possible to define which plant configurations or combination of out-of-service trains or sub-systems are acceptable, and for how long. These insights could define the bases for a set of "limiting conditions for operation" (LCOs), each of which would have an associated action statement.

### 5.11.2. Optimization of technical specifications — allowed outage times

Having defined the allowable configurations, it is also important to provide guidance on how to define an acceptable duration for a specific safety system train or sub-system. This will be derived from the PSA and then optimized to provide the greatest operating margin to the plant maintenance staff.

The unavailability assumed in the baseline PSA for each safety related system train or sub-system will be defined, and become the "bogey" for its annual allowable outage time. Importance measures for these events could be plotted into the importance measure quadrant diagram described in Figure 5-8 to identify those unavailability events which have:

- An important effect on safety assurance and risk reduction,
- An important effect on safety assurance,
- An important effect on risk reduction,
- A marginal effect on safety assurance and risk reduction.

These insights would serve to identify where allowed outage times can be increased, where they should be controlled, and where increases can only be made when compensatory measures are taken, i.e. allowed outage hours for another system train are decreased in compensation to maintain "risk neutrality".

The changes should all be optimized within the framework of the expected needs for maintenance, i.e. at the conclusion of the allocation process, the allowed annual outage hours should agree with the estimates of the maintenance experts as to how many are needed for effective surveillance testing and preventive maintenance.

When the use of on-line risk or safety monitors becomes widespread, and the plot of instantaneous core damage frequency can be reviewed within the context of the configurations which are normally encountered during operation, there should be an excellent database to use as the foundation for improved or optimized plant specifications, however, until this information is published, the deterministic approach, augmented by probabilistic estimates of the relative importance of individual restrictions on plant configuration will likely have to provide the basis for the Limiting Conditions for operation and associated action statements in near-future technical specifications.

The most comprehensive single reference which is currently available to guide the Optimization of Plant technical specifications is provided by the "Handbook of Methods for Risk Based Analysis of technical specifications", NUREG/CR-6141. This reference addresses the issues briefly describe above in great detail, and expands the discussion to include suggestions about how to optimize the test intervals and testing requirements for the plant surveillance testing programmes. This will also be of importance to D-RAP.

## 5.12. PROCUREMENT — RELIABILITY SPECIFICATIONS FOR IMPORTANT SSCs

When specifying levels of reliability, availability and maintainability for specific SSCs specifications there are several key issues which must be considered.

- **First**, the requirements should be commensurate with the needs and the expected benefits, i.e. components with high reliability are likely to cost more than those with average reliability so they should only be specified when an economic evaluation indicates the probability of a positive return on investment over the plant lifetime. This evaluation must compare the present worth of the costs and savings of the SSC offerings for each year of plant life with the initial cost differentials between offerings and select
  the one which provides the greatest net positive return after considering:
  (i) SSC reliability, availability and maintainability,
  (ii) SSC energy efficiency,
  (iii) Costs of required preventive maintenance, inspections and overhauls for SSC.

  It is important to remember that reliability and availability have no intrinsic worth. The incremental worth of increased levels of reliability or maintainability are measured entirely from their associated reductions in life cycle operational costs or averted economic risks.

- **Second**, the requirements should be realistic and when differing levels of reliability are offered by various vendors, credit should be given for differences during the evaluation process.

  Provided each vendor offering meets the minimum reliability/availability requirements, each must be considered responsive, however, additional differences in reliability between offerings should be credited in the pricing evaluation. If increased reliability provides an increased economic benefit to the plant, credit should be given in the form of a willingness to pay a premium evaluated price. Without this assurance, the vendors have no impetus to build and sell more reliable components beyond the competitive advantage that might result.

- **Third**, when SSC specifications require the vendor to provide equipment which will meet target levels of reliability and maintainability, it is essential that the request for proposal (RFP):
  (i) Clearly state that the offerer must clearly define both the levels of reliability and maintainability that the SSC can be expected to achieve throughout its life, and provide clear documentation of the information, assumptions and methods used to make these predictions**,**
  (ii) Clearly define the information which each offerer must provide in its proposal to allow the plant owner to independently assess the expected reliability and maintainability of each offering and to identify differences between offerings.

- **Fourth**, the D-RAP design team must have a technically sound procedure to guide the consistent evaluation of each offering provided in response to reliability/availability specifications for a SSC.

### 5.12.1. Evaluation of vendor offerings

There are two general approaches which may prove viable, each of which will require the D-RAP specification and procurement evaluation team members to have detailed knowledge of the functional characteristics of the hardware and its important failure modes, if the selection process is to be effective.

With the first approach, the onus of demonstrating that the SSC will achieve, or exceed the specified levels of reliability and maintainability is placed entirely on the vendor. The D-RAP team's responsibility is limited to the fair and equitable evaluation of the offerings. To facilitate this evaluation, which does not rely on blanket acceptance of the vendors' predictions of SSC reliability (MTBF) and maintainability (MTTR), the request for proposal (RFP) must include requirements which specify that the offer or include documented copies of the reliability and maintainability analyses used to establish the bases for the estimates of MTBF and MTTR provided in the proposal.

The D-RAP team will use its own knowledge of the SSC reliability and maintainability characteristics, its expertise in RAM analysis and failure investigation to review the information provided with each vendor's proposal and either confirm its accuracy, applicability and fidelity, or to modify the vendors' predictions to render them more "realistic".

With the second method, less reliance is placed on the vendor's providing its own estimates of MTBF and MTTR, and greater emphasis is placed on a prediction of the absolute and relative SSC reliability and availability by the D-RAP RAM analysis staff. To make a confident prediction of the SSC RAM characteristics requires a great deal of very specific technical information which must be elicited by the D-RAP team in its RFP.

To assure the availability of essential information needed to perform the quantitative assessment first requires the development of a failure model for the SSC by the D-RAP RAM team. This model will provides the necessary basic understanding of the SSC design characteristics which influence the rate of initiation and progression rates for individual flaws which propagate from damage state, to damage state, until functional failure occurs. It will not be until the design team has this information that it will be able to define the information set needed to perform its evaluation of the relative reliabilities for each offering.

Though the information provided by each offer or in its proposal will likely be adequate to assess the differences between offerings, it may not be possible to predict absolute values, i.e. MTBF or failure rate, with any high degree of confidence. In this case, the information provided from the RAM assessments are used to provide relative measures between offerings which are graded as below, at, or above average and calibrated in an absolute sense by failure and repair data for comparable components.

The primary difference between the first and second method, lies with the reliability and availability assessments which are performed by the D-RAP team prior to releasing the RFP with the second approach. The insights gained in this RAM assessment for a "typical" SSC are used to define the minimal set of information which must elicited from each offer or to allow independent predictions of MTBF and MTTR by the D-RAP specification and procurement evaluation team members.

Wherever possible, it may be important and advantageous to use both approaches, i.e. specify that the vendor provide both a documented basis for his predictions of expected reliability and maintainability, and the SSC specific information needed for an in-depth analysis of its reliability and maintainability characteristics by the D-RAP team. The competitiveness of the market place and the size of the potential award, is one of cost to the vendors. If the vendors do not already have a product specific database nor a RAM analysis for the offered hardware, it may be expensive and time consuming to prepare, especially if they do not have the in-house technical resources needed to support such a task. This may result in having the undesirable effects of either excessively high bid prices, or inadvertent exclusion of one or more vendors who have quality offerings.

If the entire scope of supply is not with a specific vendor, i.e. individual elements of the SSC are supplied by different vendors, it will almost always be necessary for the D-RAP team to perform a RAM evaluation which is based on information provided by each offer or.

### 5.12.2. Specification, evaluation and procurement RAM models

The most effective approach which can be used to develop RAM models specifically designed to assist in the procurement process involve the use of historical data in combination with goal Tree, fault tree or failure Mode and Effects analyses. With each modeling approach, the objectives are similar, i.e. to:

– Identify each of the functional failure modes of importance to the SSC. This task can most effectively be achieved from a review of the categorization data suggested as part of the basic SSC categorization process, and operational data sources. In the event that this information is not available, it must be derived from the RAM model.

  For a flow device, the basic functional failure modes are likely to be:
  (i) Loss of flow,
  (ii) Inadequate flow,
  (iii) Excess flow,
  (iv) Loss of flow control,
  (v) Failure of pressure boundary (external leakage).

– Take each functional failure mode and derive the hardware specific failure modes which cause it to occur, e.g. for the flow device:

Loss of flow caused by:
Torsional failure of driver, coupling, shaft, which in turn is caused by:

(a) Severe vibration induced by failed alignment or imbalance, which in turn damages bearings, causes severe misalignment and seizure or,
(b) Foreign objects, debris or internal damage caused by impeller or volute cracking and failure which causes a locked rotor, or,
(c) Failure of hydraulic thrust balancing system which in turn initiates contact between the rotating and static elements.

The above is intended to serve as an example of one, deductive, approach to SSC RAM model building. When the model is complete, so that the individual sources of flaw initiation and their propagation paths can be mapped onto the model, the analyst must ask the question, what design characteristics influence the rate of flaw initiation and propagation. The answer to this question becomes the basis for information elicited by the RFP.

For example, when there is concern for vibration induced loss of bearing life in a variable speed pump. The evaluation must first recognize that the pumps tendency to exhibit this failure mode will likely be a function of shaft stiffness, bearing design, and the proximity between the pump critical and operating speeds. This implies that the specification must specify that the offer or provide the necessary information about pump weight, bearing length to diameter ratio and bearing support systems, and the bid evaluation use this information to assess the importance of its influence on pump reliability.

The evaluations would use this pump specific information to estimate the expected effects on its reliability and assign a numerically scaled rating, e.g. +5 to –5 to approximate its importance. A value of +5 would imply that the characteristic is expected to have a very positive influence, –5, a negative influence and ‘0' implies that no correlated effect could be expected, i.e. characteristic is reliability neutral.

The aggregate rating from each defined parameter for each individual offering should provide a robust assessment of their relative reliability and how they compare to “average”. By using a typical database failure rate to represent an “average failure rate” it should be possible to estimate the probable failure rate for each SSC offering and use this in the RAM or PSA models to judge its worth and to use this worth as the basis for selecting the most cost effective SSC offering.

## 5.13. GRADED QA

The inherent problems with blanket application of quality assurance requirements for all safety related SSCs have manifest themselves primarily as producing SSCs which do not necessarily exhibit levels of reliability which are significantly higher than corresponding commercial quality items, yet cost significantly more. In the future, the application of a “graded” quality assurance programme, in which the application of “Quality Requirements” is balanced with the expected benefit and the importance of the individual SSCs, offers the promise of controlling this inefficient use of resources.

QA programmes generally focus on the imposition of institutional requirements on the procurement, manufacture, installation, operation and maintenance of all safety related components to ensure that they meet their specifications throughout all phases of plant life and during all plant activities and evolution. It is within this context that the current weaknesses in the application of QA becomes manifest, namely, that though the QA programme is focused on maximizing reliability there are generally no formal requirements to perform reliability assessments for important SSCs to provide a basis for the QA programme.

This limited viewpoint or perspective results in a tendency to focus on documentation of all activities associated with manufacture, installation and operation of the safety related SSCs, without ever exploiting current reliability engineering methods and techniques to confirm that components will provide adequately reliable operation in their selected application. This programmatic focus on meeting requirements, without regard to the formal application of reliability engineering assessments, leads to additional attributes which add to the cost-ineffectiveness of QA, namely:

- There is a tendency to subrogate responsibility for quality performance from the line organizations, to the QA organizations. This flies in the face of experience which shows that unless each line organization has responsibility for quality of its own performance, performance will never be optimal, or, in the words of an old adage "quality cannot be inspected into a product, but, must be built into it",
- QA programme focus on the blanket implementation of, and compliance with, deterministic requirements initiated to assure the quality of SSCs, decreases the freedom of RAP engineers to make decisions to implement enhancements which necessarily discriminate between important, and not so important, failure modes. Because there is a tendency to classify a complete component as "safety" or "non-safety" related, similar requirements are imposed on all piece parts, a strategy which may increase costs without necessarily increasing reliability to a commensurate level.

A "graded quality assurance" programme can be expected to have the following general characteristics:

- The QA programme will be integrated with the RA programme so that quality requirements are applied in areas where they provide enhanced reliability, i.e. reduce the frequency of flaw initiation and the rate of flaw propagation for important failure modes,
- QA requirements will be imposed upon reliability critical SSCs, and focused on prevention of the important functional failure modes to the extent that segregation of individual piece parts into those which are either safety or non-safety related, is practical within a single SSC,
- QA requirements will only be imposed upon components whose commercially available reliability is insufficient, or, components which must operate under uniquely harsh environmental conditions during the mitigation of severe accidents.

  In these cases, because there may be no actuarial experience upon which to base predictions of performance under adverse conditions, it will be necessary to:

  (i) Test the components in an environment corresponding to that which it is expected to see during an accident, and provide the necessary assurance that their "as installed" configuration and condition is comparable to the "as tested" configuration,

  (ii) Confirm that the materials of construction are as specified and compatible with the expected accident and process environment.

- The QA programme will be heavily dependent upon the RA programme because the requirements for each SSC will be derived from formal reliability analyses. The applied QA requirements will ensure that these reliability based requirements are preserved during each SSC activity initiated by the manufacturer, installer or maintainer.

The graded QA programme (GQAP) will rely heavily on the rank-ordered list of SSCs which the D-RAP team will develop and maintain current throughout the plant's design phase. The scope of the GQAP should not necessarily lead to need for discrimination between SSCs installed in "safety" systems and those within the normally non-safety related SSCs in the "balance of plant" scope of supply whose failure becomes an initiating event, and hence, may be important to safety. This fact, by implication, means that the RAM and PSA models and analytical methods and tools used to develop the rank-ordered list of SSCs must be "Quality Assured" and meet all the requirements of the plant QA programme. One general approach which could be used to develop a graded QA programme is shown in Figure 5-10.

### 5.13.1. Nominal QA requirements and the effects of graded QA

Current QA programmes rely heavily on the use of inspection, documentation and compliance auditing against specified deterministic criteria to assure the quality of important safety-related components throughout their operational life. The graded QA programme does not necessarily eliminate this approach, nor the types of activities associated with implementation of these types of programmes. A GQAP will, however, try to limit attempts to "inspect in quality" to those areas in which inspection provides an identifiable value or benefit. For example, the GQAP will:

- Identify institutional activities which influence various aspects of individual SSC reliability and exploit the insights from D-RAP to focus the definition of requirements and activities in areas in which they provide a positive payback, i.e.:
  - (a) Where material properties are known to be important, specify inspections to ensure that the manufacturer uses the required materials,
  - (b) Where piping and pressure vessel are expected to be exposed to high levels of radiation, be sure that the actual weld materials and procedures are recorded,
  - (c ) Where material integrity is important, ensure that there is an inspection record for the manufactured product, not only to provide assurance of initial quality, but, to provide a condition benchmark against which to compare the results of all future inspections,
- Implement programmatic requirements where they enhance reliability commensurate with their importance to safety, reliability or economy. In most cases, this implies that activities:
  - (i) which reduce or minimize flaw initiation and propagation rates will be controlled,
  - (ii) which do not play an important direct role in influencing important failure modes and mechanisms will be allowed to default to good industrial practices,
- Monitor procurement and manufacturing processes for original and replacement parts to ensure that they conform to original specifications-this is important to both economy and safety. However, the review will focus only on ensuring that requirements are met, where they have the potential to have a deleterious effect on important SSC failure modes, e.g. assume commercial bolting on a pressure boundary seal is adequate, when the nominal specification with commercial quality is adequate.

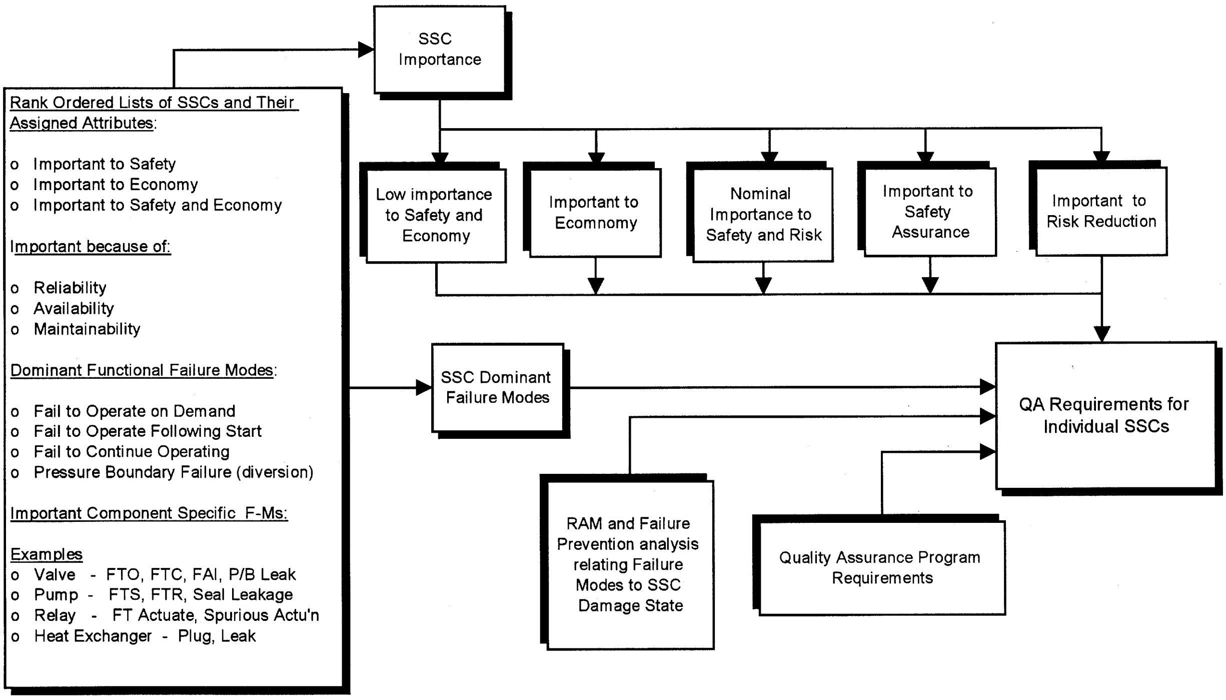

SSC Importance
Rank Ordered Lists of SSCs and Their Assigned Attributes:
o Important to Safety
o Important to Economy
o Important to Safety and Economy
Important because of:
o Reliability
o Availability
o Maintainability
Dominant Functional Failure Modes:
o Fail to Operate on Demand
o Fail to Operate Following Start
o Fail to Continue Operating
o Pressure Boundary Failure (diversion)
Important Component Specific F-Ms:
Examples
o Valve - FTO, FTC, FAI, P/B Leak
o Pump - FTS, FTR, Seal Leakage
o Relay - FT Actuate, Spurious Actu'n
o Heat Exchanger - Plug, Leak
Low importance to Safety and Economy
Important to Ecomnomy
Nominal Importance to Safety and Risk
Important to Safety Assurance
Important to Risk Reduction
SSC Dominant Failure Modes
QA Requirements for Individual SSCs
RAM and Failure Prevention analysis relating Failure Modes to SSC Damage State
Quality Assurance Program Requirements

*FIG. 5-10. Use of rank-ordered SSCs in graded QA.*

The importance of GQA in future reactors will depend, to a large extent, to the degree to which formal D-RA and O-RA programmes are used to specify the plant wide reliability specifications for SSCs. When the specification of all SSC requirements for reliability are dictated by the RA programme, the QA programme should be applied in all areas of importance to confirm that the specifications are being satisfied, in other words, QA requirements are dictated by the RA programme to proved GQA by default.

Where comprehensive implementation of plant-wide D-RAP and O-RAP does not occur, the ad hoc reduction in QA requirements for individual SSCs, typical of current approaches to "graded QA" will reflect the insights above and will be guided by RAM and PSA assessments wherever possible and practical.

Note:
At all times, deterministic QA requirements imposed by the cognizant regulatory authorities in individual member states must be waived or modified before insights and directives from D-RAP and O-RAP can lead to any relaxation of current QA requirements.

## 5.14. ENVIRONMENTAL QUALIFICATIONS

It is important that the reliability assurance programme provide guidance on the needs for environmental protection and environmental qualification for important SSCs, for both acute and chronic exposures to hostile environments. D-RAP will facilitate achievement of this objective by combining the results from detailed severe accident thermal hydraulic and fission product transport analyses for the plant reactor and auxiliary buildings and the results from the level 2 containment analysis to:

- Identify each plant area or compartment which contains risk important equipments or their support systems, cables, buses and piping and,
- Establish a minimum set of environmental criteria which each SSC must be able to withstand when operating within these areas identified areas.

D-RAP will then use insights about the possible failure modes for each of these important SSCs to guide the development of specifications which the manufacturer must satisfy to minimize the initiation and progression rates for these failure modes under the specified accident conditions. An important role that D-RAP can play in defining EQ requirements is one of allowing flexibility in the configuration of field terminations and in the manufacturing of the equipment to standards which are specifically aimed at enhanced reliability, and minimizing reliance on rigid deterministic requirements which may, or may not, actually enhance SSC reliability.

D-RAP can play a second key role in the area of EQ, namely, in the determination of allowed life for individual piece parts. The reliability assessment for important SSCs will not only provide insights about the failure modes, but the piece parts whose degradation can accelerate their rates of progression. When the effects of both acute, and chronic, environmental stress on these mechanisms and failure modes are assessed, it should be possible to determine those which are subject to important ageing effects and those which are not. Though perform such a detailed analysis for all important SSCs and their associated hardware (instrument loops, actuation systems, cooling systems, cables and conduits) may seem like an overwhelming task, similarity in the construction for representative types should enable the maximum use to be made of "generic models", from which insights can be inferred for specific cases.

When the individual piece parts which both age in the specified environments, and whose condition is important to the prevention of important failure modes, are identified, the D-RAP team can confirm the appropriateness of any replacement schedules suggested by the manufacturer, or in its absence, define the necessary requirements.

### Environment qualification for SSCs important to safe shutdown

Though the risk assessments and safety analyses can provide a quantitative basis for assessing importance and conditions for individual SSCs during severe accidents, it is also important to recognize the need for maintaining the availability and reliability of components which are required for safe plant shutdown and that these components are qualified for their long term operating environment. This "safe shutdown analysis" is generally not part of the RAM or PSA scope of activities, but is intended to provide a deterministic assessment of the adequacy of normally available success paths which can provide the needed critical plant functions during a plant shut down after the occurrence a specified casualty or SSC failure caused by a transient, loss of offsite power, loss of RCS integrity, an internal fire, flood or other condition which has a major impact on the availability of plant systems.

For each accident initiating event which is identified by the PSA, there is an implicit assumption that provided the fuel clad is protected for a specified period of time, the plant will shut down safely. The safe shutdown analysis is one of the ways that this premise is confirmed, albeit generally in a way which is independent of the PSA.

It is important that the EQ programme include consideration of the accelerated ageing effects from long term operational exposure to mildly hostile environments do not result in premature failure of SSCs which are important to plant shutdown, yet perhaps of marginal importance to safety.

The "pro forma" extension of the reliability assurance programmes to include these components should be routine.

## 5.15. INVESTIGATIVE METHODS

### 5.15.1. Reliability, availability and maintainability improvement (RAMI)

Consistent with the definitions provided earlier in this guidebook, the term "RAMI" is used here to imply RAM "improvement", as distinct from the more general, and commonly used term, RAM, which refers to reliability, availability and maintainability.

A general description of RAMI and how D-RAP can be exploited to achieve RAMI in the design process has been provided earlier in sections 2 and 3 and in the descriptions of the individual D-RA programmatic activities discussed in this section of the guidebook. Though it seems that the differences between RAMI for design and operations are large, in reality, they are functionally quite similar. The primary differences result from the need to use analytical techniques to predict potential problems while the plant is in its design phase, whereas during operation there will generally be a great deal of available empirical and actuarial data with which to pin point problems.

During the design phase, results from the RAM analyses provide the information base needed to effect enhancement activities, whereas during the mature years of plant life, operational experience provides the necessary information base. In the interim, i.e. during the first few years of plant life when operational experience is accumulating to the point that it represents a complete picture of plant performance, a combination of prediction and data collection and analysis will serve to identify important areas in which generation losses are increasing and to provide the information from which their causes can be inferred.

### 5.15.2. D-RAP and availability improvement

In a simplistic sense there are only two issues to be resolved during the development of an availability improvement or optimization process during design:

- **Where** best to attempt improvements in availability or productivity,
- **How** to effect improvements in availability when areas which merit attention have been identified.

Finding an appropriate answer to these questions, however, can be quite difficult and the solutions to the many problems which result in loss of availability are frequently not obvious. If proposed changes to the plant are not technically well founded within the total plant environment, expected improvements are often not fully realized. In some cases, proposed changes may even introduce new problems which are only slightly less troublesome than those being corrected.

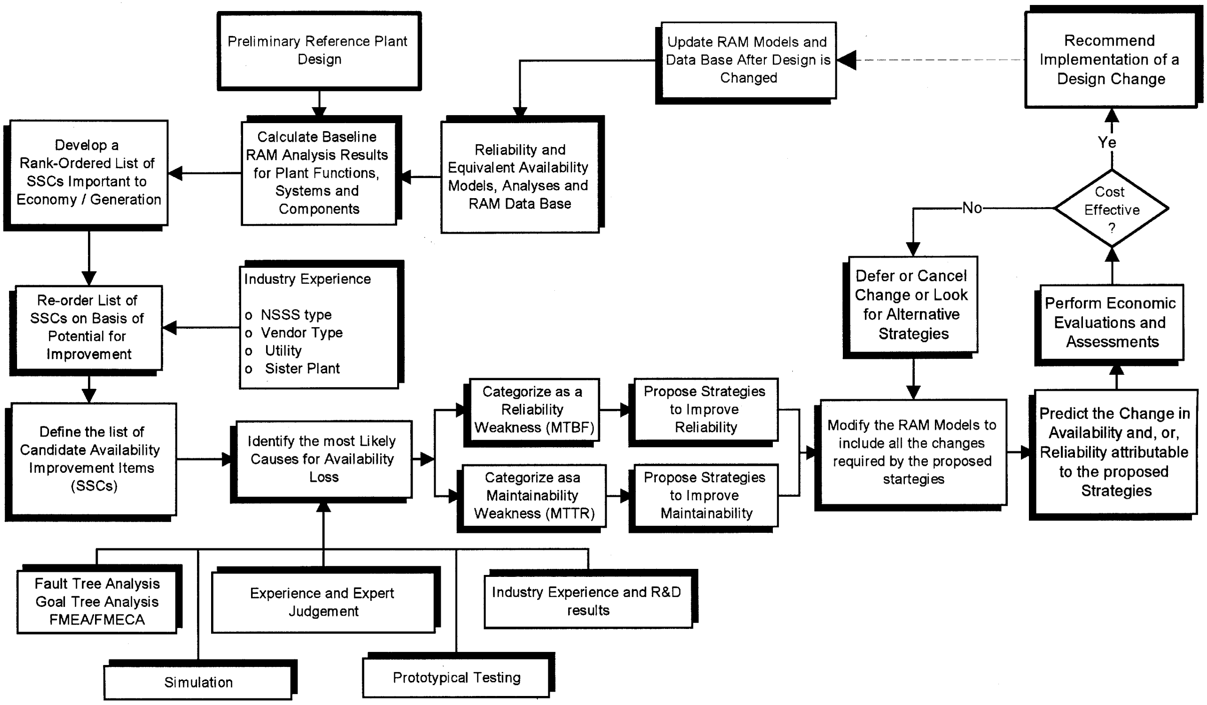
The inherent complexity of the power generation cycle requires that for constant and continuous improvement, the plant designer and owner/operator must apply a formal, consistent and comprehensive approach towards availability enhancement and fully integrate all plant activities which lead to the achievement of optimal availability. The individual activities necessary to ensure an integrated, adequate and effective programme will be discussed within the context of the overall availability improvement process shown in Figure 5-11.

### The availability improvement process

There are three distinctly different activities at the heart of the availability improvement process:

- Identification of an ordered list of candidate availability improvement programme (AIP) items, i.e. a prioritized list of components/things in the plant which probably should be fixed,
- Identification of effective changes or remedial actions for each candidate AIP item which will either reduce its failure frequency or reduce the time required to restore it to functional operability following a failure, i.e. a set of recommended actions or activities which will improve the reliability or maintainability of each of the components/things on the AIP list,
- Justification and prioritization of each candidate AIP action on the basis of cost benefit comparisons, and optimization of the implementation schedule within the time (schedule), manpower and budgetary constraints which are inherent to any industrial activity, i.e. a way of prioritizing the implementation of plant changes so that the owner will get the quickest investment return.

Each of these elements or programmatic activities will now be described in more detail.



Preliminary Reference Plant Design
Update RAM Models and Data Base After Design is Changed
Recommend Implementation of a Design Change
Develop a Rank-Ordered List of SSCs Important to Economy / Generation
Calculate Baseline RAM Analysis Results for Plant Functions, Systems and Components
Reliability and Equivalent Availability Models, Analyses and RAM Data Base
Ye
No
Cost Effective ?
Industry Experience
o NSSS type
o Vendor Type
o Utility
o Sister Plant
Re-order List of SSCs on Basis of Potential for Improvement
Defer or Cancel Change or Look for Alternative Strategies
Perform Economic Evaluations and Assessments
Categorize as a Reliability Weakness (MTBF)
Propose Strategies to Improve Reliability
Define the list of Candidate Availability Improvement Items (SSCs)
Identify the most Likely Causes for Availability Loss
Modify the RAM Models to include all the changes required by the proposed startegies
Predict the Change in Availability and, or, Reliability attributable to the proposed Strategies
Categorize asa Maintainability Weakness (MTTR)
Propose Strategies to Improve Maintainability
Fault Tree Analysis Goal Tree Analysis FMEA/FMECA
Experience and Expert Judgement
Industry Experience and R&D results
Simulation
Prototypical Testing

*FIG. 5-11. RAMI in design.*

### 5.15.3. Development of an ordered list of candidate AIP items

Three elements are key to the development of an ordered list of candidate AIP items:

(a) A benchmark historical database which provides a list of significant contributors to unreliability and unavailability for similar plants, in terms of:
   (i) SCRAM and full forced outage rate,
   (ii) % Equivalent Unavailability and capacity factor,
   (iii) MW/h lost generation per year,
   (iv) $ cost of purchased fuel and energy charges,
   (v) Plant heat rate-important because the regulatory limit on reactor (thermal) power means that any degradation in efficiency will appear as a source of plant equivalent unavailability,

(b) Information which describes levels of component reliability and maintainability seen for SSCs which are similar to those in the ALWR under analysis,

(c) Plant reliability, availability and cost models which provide the linkage between individual component performance characteristics (reliability, maintainability) to overall plant performance (equivalent availability, SCRAM rate and economy).

Combination of each of these elements into a comprehensive quantification technique which can be used routinely to support design decision making, gives the RAM engineer with the tools needed to determine where design vulnerabilities may exist, and how these failures can potentially effect the overall plant economic mission, and by how much.

**Equivalent availability or availability**

There is a difficult question which must be resolved early in the development of RAM models for design, and that is, whether a single availability model can be used. An availability model uses “success criteria” to define the logical relationships between the individual capabilities of plant SSCs and the achievement of the overall plant missions and quantitative performance. The model shows all redundant, diverse and individual hardware and human elements which are part of a success path needed to support the generation process functions.

Because electric generation systems can exist in any one of a number of possible discrete success states, when a capability is increased from minimum to maximum, use of a single RAM model is no longer appropriate. A set of RAM models, each of which has success criteria which correspond to a specific success state, must be present. A single operating availability model can be used to estimate the average probability that the plant will successfully achieve minimum load (the lowest order success state) throughout a defined operating period, but, this parameter cannot be directly linked to its economic worth so it has limited applicability to the D-RAP design process.

This leads to the use of multiple models whose individual power state results are combined graphically in a cumulative distribution function of "the probability of exceeding capability X" vs. "capability X". Integration of this curve provides the plant equivalent availability which, when combined with the expected load curve and generation economics, allows direct calculation of expected generation and revenue. Prediction of equivalent availability is essential when seeking justification for a proposed modification which does not effect the probability of success at either maximum or minimum plant load. For example, when assessing a proposal to increase pump capabilities, the only effect may be at intermediate power levels, but if the plant operates in these regions for a significant period of time, a real financial benefit may result.

**Reliability models**

Prediction of SCRAM rate and plant full forced outage rates requires the development of a “reliability model” whose quantification provides the frequency with which a Reactor Trip or Plant shutdown will occur. Reliability models are typically fault oriented and deductive in nature, i.e. developed and quantified using fault tree technology, however, use of success orientation can sometimes provide additional insights since the focus also includes explicit consideration of the possible ways to “prevent damage to SSCs” from the many fault conditions which may occur.

The reliability model will identify, in hierarchical fashion, the protective functions which must be maintained during normal operation, i.e. those for which SCRAM or immediate shutdown is initiated, and the hierarchy of faults, within and outside the protective systems which serve to trigger the shutdown sequence.

Because the fault tree has the potential to include both initiating events (the trigger failure) and subsequential or consequential failure events, quantification will involve the assignment of both frequencies and probabilities to them. Because the fault tree will predict “frequency of SCRAM” it is ESSENTIAL the event naming and identification system be extremely precise so that all event conditionalities are preserved.

The results from the reliability analysis will be a set of rank-ordered SCRAM or shutdown sequences (initiating event and subsequential or consequential failures) and a set of importance measures for individual SSCs. To predict the plant outage rate, these shutdown sequences will be grouped by similarity in impact (expected plant mean down time) and their aggregate values used to find the contribution from each group. Group frequency (shutdowns/a) times impact (hours/shutdown) gives the forced outage contribution from each group, and the sum of the contributions from each group, provides the impact at the plant level.

**Relating performance to economics**

The primary role of the plant availability models is to provide the cause and effect relationships between proposed plant changes and the resultant effect on plant performance. Having this capability allows an analyst to determine the expected cost benefit for all proposed modifications, and provide the needed justification and priority for implementation.

The model has a strong secondary role by providing the individual contributors to equivalent unavailability in rank order, so that areas of vulnerability can be identified and used to identify preliminary AIP candidates. This is a particularly important attribute during the development of a new plant availability improvement programme, when little historical data or experience is available.

**When, and when not to "model"**

The answer to this question is that a "model" is always needed, but the necessary scope and detail of the model may differ dramatically as various issues are explored. The range of models can span the gap between a simple data model in which only broad functional elements are included, and a complex, highly detailed multi-state model which includes dynamic interrelationships, human activities and explicitly linked support systems.

“The correct model is the one which provides the most appropriate answers to each question which is posed, with minimum expenditure of available resources”.

Typically, models built to support an AIP programme tend to be rather complex so that they will maintain general applicability. If the initial model scope is too limited, the model may require reconstruction or continuous modification to answer each new and different question. This situation can lead to unnecessary rework and may be avoidable when the analysts use reasonable and justified modeling criteria.

### 5.15.4. Databases

A plant specific database plays an essential role in the AIP by providing the foundation for:

- Expected or predicted component or subsystem failure probabilities in the equivalent availability models,
- Predicted plant mean down times for specific SCRAM or shutdown events,
- An initial assessment of the relative and absolute importance of individual SSCs and the areas in which the D-RAP AIP should be focused,
- “Sanity” checks on predictions of SSC performance. Models may predict unrealistic performance levels for SSCs if founded on ill-conceived assumptions. Comparison of predicted with historical data can serve to check the unbridled use of RAM model results, without first achieving an understanding their limitations and inherent uncertainties.

A truly plant-specific database will not be available to a plant in the design process, so its equivalent must be generated from other non-plant specific sources, i.e. the D-RAP team must develop a database which is appropriate to the new plant design from generic, yet applicable, industry databases. This is very important because this failure rate and repair time information contained in this database is relied upon to provide:

- Surrogate component performance data for new plants, from which there may be very little experience to infer component reliability and maintainability,
- A basis for including “potential for improvement” as one of the priorities used to rank order the RAM model-generated AIP candidate list.

In judging the “potential for improvement” a comparison is made between predicted SSC performance and the level of industrial typically experienced by comparable SSCs. The results from this comparison are used when an SSC is predicted to be a dominant contributor to plant unavailability or unreliability, yet its predicted performance is at industry “norms”.

The results from the comparison between historical and future expected performance may imply that unless the SSC can be re-designed or known faults can be corrected, the potential for real improvement is small. In this case, reprioritizing the list may be appropriate to prevent expenditure of valuable design resources in areas which have limited promise for a positive pay-back. This may also be a case in which the benefits from additional redundancy or diversity should be actively assessed by the D-RAP team.

### 5.15.5. Changing SSC performance

The RAM modeling processes provide rank-ordered lists of SSCs whose reliability and availability are important to generation, and provides a measure of the worth of an increase in SSC reliability and maintainability. The question facing the designer is one of how best to effect an improvement. Remember, if improved reliability and availability were easy to achieve, in all likelihood, the manufacturer of the SSC will already have attempted to achieve it!

When SSC performance improvement is sought, reductions in failure rate and mean down time are both viable options. This is because:

- Availability, the average probability that the SSC will be in a successful operating state during a specified period of time, is one of the most important measures of hardware economic performance,
- Availability is a function of both SSC reliability (failure rate) and SSC maintainability (time to restore following a failure),
- Reliability of SSCs is important when their failure can initiate a SCRAMs or plant shutdown because a SCRAM or shutdown results in a loss of generation and in its becoming potential accident initiating event which affects both economic risk and safety,
- SSC maintainability and plant operability and maintainability is important to minimize the average down time following a SCRAM or shutdown and its contribution to full forced outage rate.

The above implies that the first step in the availability improvement process becomes one of understanding and identifying the causes of unavailability, and where the potential for improvements is likely to be most profitable.

Note:
If component failure leads to dynamic system behavior which in turn initiates total system failure and a plant trip or shutdown, generation lost during restart may dictate that component reliability becomes the primary focus, particularly if the restoration time for the component is less than the time required to restart the plant. If component failure merely leads to operation at reduced capacity, reduction in component mean down time may be just as important as failure rate.

For the above reasons, attempts to improve component performance must include examination of both reliability and maintainability options. However, the primary focus must be determined on a case specific basis.

### 5.15.6. Reliability and maintainability requirements for all SSCs

Though, from the descriptions provided below, the focus of the availability optimization process may seem to be limited to incorporating reliability and maintainability requirements into the design of important SSCs. These same activities must be performed for all SSCs, regardless of importance. The “good industrial practices” used to design, select, procure and install SSCs of lesser importance MUST reflect consideration for these same design principles.

The primary differences between the gradations in RA programme requirements for SSCs come from their importance and reflect the lengths that the designer may be justified in taking to achieve his objectives. The potentially high economic benefits from improvement in performance of important SSCs will influence design decisions which allow the specification of "non-standard" hardware characteristics which are different from those of generally offered by the vendors of commercial hardware.

The other important issue may be that, for items with very low importance, there may be little justification for performing detailed reliability or maintainability analyses of vendor offerings. Provided each vendor offering meets the functional specifications defined in the RFP, price may be the dominant determinant in the selection process.

The design for all SSCs should be reviewed against a checklist of requirements and good practices to confirm that none have been overlooked, and that all decisions which result in less than optimum SSC reliability, availability and maintainability are made deliberately.

## 5.16. IMPROVING THE PERFORMANCE OF IMPORTANT SSCs

The D-RAP team must make use of the programmatic tools described in detail elsewhere in this guidebook, but to recapitulate the possible options, the D-RAP team should:

- Use the D-RAP RAM modeling and analysis process to produce the categorized and ranked list of SSCs which are important to plant reliability and economic performance,
- Use the categorization process to focus their attention on the issues which are important to the improvement process and have a realistic potential for gain, or offer a positive return on the invested resources,
- Define the issues of importance to the D-RAP improvement or enhancement process for each important SSC:
  (i) Failure modes of importance,
  (ii) Whether failure mode importance is a result of reliability (failure rate) or maintainability (time down for test, repair, inspection or overhaul),
- Assess the potential for enhancement of reliability and or maintainability, by comparison with historical experience for similar SSCs operating under similar conditions,
- Define a D-RAP strategy for the reliability, availability or maintainability enhancement process for each important SSC.

### 5.16.1. Reliability enhancement

To enhance the reliability of individual SSCs and minimize the number of unplanned functional failures, the cognizant designer should:

- Use a combination of historical records from past failures and a focused reliability assessment for the SSC, e.g. goal tree or equivalent, to identify:
  (a) Dominant functional SSC failure modes,
  (b) SSC flaw initiating mechanisms and likely initiating sites,
  (c ) Intermediate SSC damage states and failure propagation paths which, without
  (d) intervention, culminate in the functional failure of the SSC,

(e) Environmental and process conditions which influence the rates of flaw initiation and progression, and an estimate of the relative progression rates for each important failure mode,

(f) Information which is potentially available to diagnose SSC damage state and infer SSC internal condition,

- Use information from the SSC reliability assessment to guide the specification of materials of construction and manufacturing methods to minimize the probability of flaw initiation and propagation for important failure modes,
- Use information from the SSC reliability assessment to develop an effective protective actions strategy which not only prevents catastrophic failure (long down time) but also does not result in premature or spurious shutdowns (high shutdown rate):
  (i) Define information which can be feasibly collected and analyzed to infer internal SSC condition, or, severe external threats to its condition from the process, and construct an intervention strategy which can be used to initiate automatic or manual protective action,
  (ii) Develop a highly reliable automatic strategy (highly redundant) which will ensure immediate cessation of damage state progression and prevent consequential damages for important failure modes, yet minimize vulnerability to spurious shutdowns caused by false inputs or failed actuation devices in any one of the redundant paths, i.e. develop an M-out-of N logic which achieves both highly reliable operation without susceptibility to spurious actuation,
  (iii) Develop an effective diagnostic and monitoring package which will guide the operator’s decisions about SSC shutdown in the presence of deteriorating internal conditions or severe external threats to its integrity.

**General philosophy for protective systems**

SSC shutdown systems either initiate an automatic trip or annunciate a warning whenever the protective system detects unacceptable internal hardware conditions or the presence of potentially damaging external threats. In principle, an equipment protective trip contributes to SSC availability by preventing the occurrence of severe failures and their attendant demands for long down times to effect repair, at the expense of more frequent shutdowns when the SSC remains in a relatively benign, or less severe, damage state.

A protective system provides higher SSC availability by providing a large decrease in average down time at the expense of a small increase in effective failure rate.

The need for protective systems is generally driven by the cost and complexity of the protected equipment, i.e. protective trips are standard on turbines, generators, reactors, large pumps, fans, motors and electrical equipment.

Where standby safety related equipment must operate on demand during an accident, and repairability is not of value nor concern, equipment protective systems may not be installed because there is little opportunity for a positive return yet there may exist the potential for a large negative return if a spurious or inadvertent SSC trip were to occur.

### 5.16.2. Maintainability enhancement

To enhance the maintainability of individual SSCs and minimize the average down time following unplanned failures, or, to minimize the contributions to unavailability from test and preventive maintenance activities, the cognizant designer should follow the general precepts described in section 2 and summarized below.

When the SSC categorization process indicates that maintainability of normally operating components is important to plant forced or planned outage rates, the cognizant designer should first separate the contributions to SSC unavailability from preventive maintenance and testing from the contributions associated with corrective maintenance and planned overhauls because they require different treatment.

### 5.16.3. SSC unavailability from required tests, inspections and PMs

The primary goals of the designer when designing, specifying and selecting SSCs whose down time from required tests and inspections makes important contributions to SSC unavailability, are to:

- Minimize the need to interfere with normal operation by providing effective on-line diagnostics which allow the maintenance staff to use condition directed maintenance, in lieu of periodic tests and inspections.

The SSC reliability analysis can provide the insights about hardware failure characteristics which are needed to guide development of a programme of this type.

- Perform a formal assessment of the risks which are accepted if the plant elects not to comply with equipment manufacturers recommendations for on-line testing of critical equipment, and confirm that the testing is, or is not, cost effective. This type of assessment may be important when determining how often to test turbine stop valves.

This type of assessment should consider each of the following contributors when assessing cost benefit ratios for a specific testing activity:

Costs of test:

- Loss of generation per test, if load reduction is needed

Loss of generation = tests/a * reduction in MW/test * duration of test

- Expected loss of generation per test if a load change or other associated activities have the potential to cause a SCRAM

Expected loss = tests/a * P[SCRAM | test] * generation lost/SCRAM

**Benefit from test**

Reduced economic risk attributable to the test
$risk = {failure rate/a | no test — failure rate/a | test} * $consequences of failure

A difficulty may arise when trying to assess the effects of testing on reliability, because there is seldom a clear-cut quantitative relationship between them. In this case, the designer should use judgement and experience to bound the issue and make the necessary decisions.

– Maximize the testability of the SSC, i.e. make sure that where feasible and justified:

  (a) Connections needed to either test the SSC, or to monitor its performance during the test, are provided. By minimizing the number of required temporary connections the error rate associated with configuration induced system transients should be minimized,
  (b) The system is designed to accommodate testing, to the maximum extent possible by providing adequate permanently installed test instrumentation.

– Minimize the down time required for preventive maintenance activities:

(a) Review the preventive maintenance requirements provided by the equipment vendor and compare them with the insights and results from the reliability assessments performed for the SSC,
(b) Determine the value of the suggested PM activities in preventing the occurrence of important failure modes and identify those which can be expected to be effective,
(c) Review the design of the SSC and identify any feasible changes which will enhance the performance of the proposed preventive maintenance activities,
(d) Based on the results from the above, define the requirements for on-line PM, both in terms of applicable maintenance actions, their periodicity and if possible, modify the specifications or design to minimize the time required to effect the required maintenance actions.

### 5.16.4. SSC unavailability from required corrective maintenance

To minimize the down time required to repair, replace or refurbish a failed SSC, the designer must optimize the design to cost effectively reduce each individual contribution to down time by minimizing the design contribution to:

– Pre-repair delays,
– Delays and inefficiencies incurred during performance of the repair task,
– Post-repair delays.

*5.16.4.1. Pre-repair delays and inefficiencies*

To minimize the pre-repair delays the SSC designer should review the design to confirm that it meets all of the maintainability criteria which should be considered for all plant hardware, namely that:

– The area surrounding the SSC is laid out in a manner which facilitates radiation surveys which may be needed prior to initiating the repair process,
– Tag-out, drain and de-energization boundaries are reviewed to confirm that requisite connections are provided in locations which are both accessible and functionally viable, e.g. pipe vents which must be opened to drain system piping are both accessible, and at high points in the pipe, and that drain are at the low points and close to a plant drains so that long lengths of temporary hoses are not needed. Where systems may contain contaminated or radioactive fluids, confirm that there is ready access to the plant liquid waste systems,

- Chain or reach-rod operators are installed on inaccessible manual valves and they are oriented so that they can be easily operated from the compartment deck or access ways,
- Clearly visible, standard nomenclature, equipment tag identifiers are provided with each isolation boundary component to speed their unambiguous identification,
- Equipment or plant instrumentation provides enough information to allow effective diagnosis of the failed SSC damage state to facilitate maintenance repair pre-planning and staging activities,
- The areas surrounding the SSC contain no interferences from other systems which must be removed before repairs on the SSC can be initiated. This includes confirmation that there is adequate clearance for removal of rotating machinery internals, and that piping or cable runs from other systems do not interfere with SSC disassembly or removal,
- Special rigging points, anchorages or monorails needed to disassemble or remove the SSC are pre-installed and that interferences, e.g. cable trays or small bore and field run piping, do not interfere with the ability to use them,
- Rails or rollers are permanently installed for heavy equipment which must be moved out of place for repair or overhaul,
- SSCs installed in a high radiation area are shielded to preclude the need to install it prior to initiating a repair,
- Any needed support systems, such as breathing air, plant air (for tools), and welding and power receptacles are provided in the vicinity of important SSCs to minimize delays because of the need to set up temporary wiring connections and hoses before the repair process can be initiated,
- Evaluate the feasibility of installing catwalks or permanent scaffolds where they may be needed to gain access to the equipment during disassembly or repair.

*5.16.4.2. Repair delays and inefficiencies*

The designer should review the design and proposed installation to confirm that:

- The equipment is installed in an area which has adequate lay down space and sufficient available access for both the maintainers and their equipment,
- The SSC diagnostics are sufficient to allow effective staging for the repair of the dominant functional failure modes. “Staging” includes preparation of procedures, collection of needed tools, parts and special equipment and the definition of any needed personal protective equipment, e.g. anti-contamination suits, respirators, plastics or air-hoods,
- A reasonable work environment is provided, i.e. ventilation, light, heat, radiation protection in each area which is likely to be an important source of maintenance activities. Inadequate environmental controls either result in worker inefficiencies, either because they must wear excessive amounts of personal protective equipment or initiate delays while temporary utility services, e.g. portable fans and temporary lights are established,
- Provide elevators and open walkways wherever possible to provide maintainer access to and from the job site with needed tools and equipment, and minimize delays incurred when traveling to and from the workshop to get additional tools, parts, etc.
- SSC protective instrumentation and actuation systems are designed to detect, diagnose and actuate shutdown, or warn the operators, before important failure modes can progress to the point where consequential internal damage results, i.e. control the damage to minimize the scope of required repairs,

- The equipment is inherently maintainable, i.e. can be disassembled and repaired in the field. This is particularly important for hardware which may become irradiated or contaminated to a level which precludes its being shipped off-site or even to the main plant repair facility,
- Exploit the results from the reliability and maintainability analyses to define an adequate, yet cost effective, set of equipment spare parts and replacement assemblies which can be provided as part of the initial SSC purchase, and prevent delays when needed spares are not available on-site.

#### *5.16.4.3. Post-repair delays and inefficiencies*

Many of the hardware characteristics associated with minimization of post-repair delays are similar to those suggested above to minimize pre-repair delays, i.e. access to the SSC boundary isolation devices, primarily valves, which must be manipulated to reestablish equipment operability. However, following repairs, there are often requirements to perform a functional test before the SSC is returned to service. The ease with which this test can be performed can have an important effect on the time required to complete it. The designer should try to minimize the time required to perform post-maintenance tests and:

- Use the insights from the SSC reliability analysis to guide development of a pre-test examination which will identify potential problems which may follow improper maintenance, or the installation of inadequate, defective or incorrect parts. Having an effective tool of this type will:
  (i) minimize the probability that an improperly performed maintenance activity will remain undetected until the functional test,
  (ii) reduce the probability of a functional test failure which requires repetition of the isolation, repair and de-isolation process.
- Design the installation to allow complete “off-line” functional operation of the SSC, e.g. ensure that there are adequately sized recirculation lines for a standby pump so that it can be operated and tested without having to inject flow into the normal process and without having to establish a temporary alignment, which itself must be restored at the completion of the test.

## 5.17. RISK BASED DESIGN OPTIMIZATION

The use of risk based tools to optimize the design of the ALWR, follows a process which is very similar to that used by the RAMI programme to enhance plant economic performance. The D-RAP will provide a set of reliability, containment and risk models, whose development parallels the evolution of the plant detailed design. The models are continuously updated and requantified to match the increasing specificity and detail of the plant design so that the D-RAP team can use them to provide:

- Overall assurance that the evolving design continues to be capable of meeting the prescribed quantitative objectives, at the plant, function and success path or system levels,
- Continuous feedback to the design team about the effectiveness of their evolving design,
- Identification of the absolute and relative importance of individual SSCs (systems, structures and components) which influence plant risk or plant safety in some way, during each operational mode of concern,

- The importance of external initiating events and structures and plant characteristics which present the greatest threats to SSC vulnerability,
- Insights into the overall plant risk profile and confirmation that the risk is not dominated by a single, or limited set of, accident sequences with the same initiating events or failed SSCs, i.e. the plant risk profile is "flat",
- A technical basis for the development of risk based strategies to optimize the design, i.e. meets all prescribed deterministic and probabilistic criteria imposed by either regulatory or industrial organizations, at minimum life cycle cost,
- Guidance in the definition of the plant information systems which are needed by the operating staff to diagnose, manage and recover from important plant damage states which may follow the occurrence of an internal or external initiating event,
- A rank-ordered list of SSCs whose absolute and relative importances which can be used to guide the implementation of risk based goal setting, optimization of the design of the plant support system infrastructure, and focus the designer's attention on development of reliability, availability and maintainability assessments for individual SSCs, where they are most justified,
- A rank-ordered list of important severe accident sequences and the local conditions which are predicted by deterministic containment models to guide:
  (i) the specification of appropriate environmental specifications for hardware which must operate in a hostile environment during severe accidents,
  (ii) Definition of information requirements which the designer must satisfy to facilitate the implementation of severe accident management strategies,
  (iii) Define the scope and character of plant severe accident behavior which the plant simulator must be designed to handle.

Though the quantification of these models cannot take advantage of a plant-specific operational database, a surrogate for this database will be constructed form all available sources of failure and repair data which is appropriate to the design. As the design matures and the details become evident, the database, along with the PSA models, will be periodically updated to assure the highest possible levels of accuracy and fidelity.

### 5.17.1. PSA development and use during design evolution

During the design phase, an evolving series of PSA models will be used to support D-RAP as the plant design evolves and details become better defined. One possible evolutionary path for PSA model development is presented below. Though this description may not exactly match the needs of any specific design programme, it does portray the full range of available options, together with an indication of their applicability at various stages of design. This section of the guide does assume that the PSA will initiated at the onset of the design process, when there is complete freedom to make changes wherever needed to modify the plant risk profile, or optimize costs within the constraints imposed by the applicable deterministic criteria defined by the licensing authorities.

In all likelihood, this will seldom be possible for a prospective nuclear plant constructor, because pre-certification of the designs offered by each NSSS vendor will probably result in their being very much "fixed" at the time of commitment. As a result, the user of this guide should merely "jump into" the evolutionary path wherever it is appropriate to the specific situation. The user should however, examine the characteristics of each described PSA product, because, though not necessarily required for D-RAP, some products may provide valuable insights which provide peripheral perspectives which are extremely valuable.

One very important issue to always bear in mind, for D-RAP to really effect change in the design process, the PSA models must be “living”, i.e. able to change quickly to both adapt to new decision making needs and to reflect the “as is” design configuration as it evolves. The use and character of the PSA must NOT become institutionalized and immutable, otherwise it will become just another burden for the design team to bear, as proceduralized “form” becomes more important than “substance”.

### *5.17.1.1. The master plant logic diagram (MPLD)*

Initially the PSA model will lack explicit detail and represent the fundamental reliability structure of the plant, probably in the form of a functional hierarchy because this can be developed without concern for its ability to match the ultimate plant design. A master plant logic diagram (MPLD), similar in construction to that shown in Figures 5-12A and 12B, or its equivalent, can fulfill this role and serve as extremely useful adjunct to the design because its high generic content allows rapid development, i.e. an MPLD for one PWR (BWR) looks similar to other PWRs (BWRs), at least to the point that individual success paths emerge from the design. Because the MPLD provides a visual display of each logical relationship which will eventually be part of the PSA, it also allows non-specialists to understand the qualitative risk importance of individual aspects of a risk based design process. Several sources of information on the MPLD concept are provided in the bibliography.

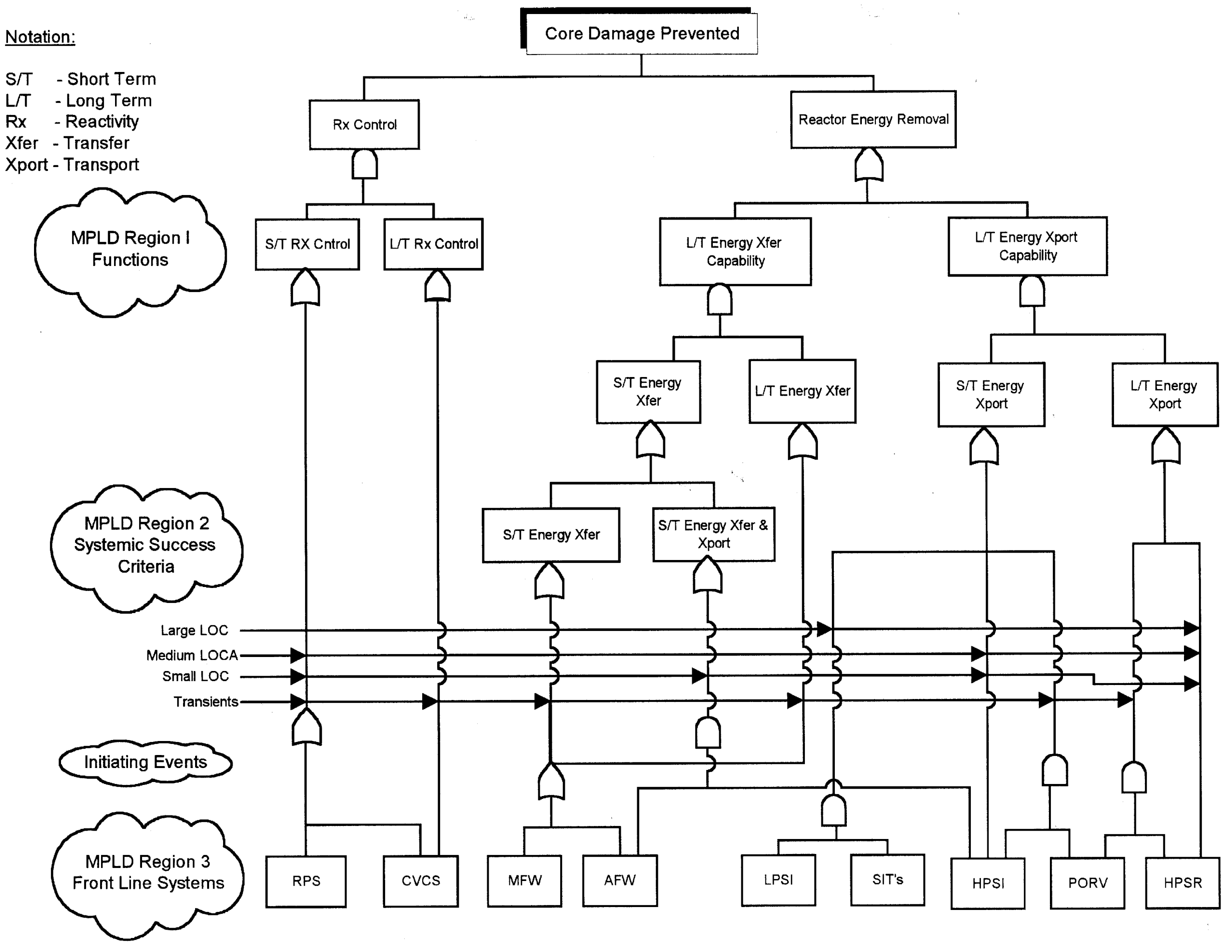


*FIG. 5-12A. Master plant logic diagram (functional logic).*

During the past few years, a great deal of resources have been expended in the rigorous performance of nuclear plant probabilistic safety assessments (PSA). These analyses provide an excellent foundation for risk based decision making, but tend to have several inherent disadvantages. They can be complex, difficult to understand by the non-specialist user, and frequently require the use of extensive computer file manipulations before they can be used to answer specific operational questions. In an attempt to overcome some of these inherent communication difficulties between the analysts and non-specialist PSA users, a new type of model has arisen. The MPLD is designed to provide a visual display of all of the detailed plant system inter-dependencies which are important to, or affect plant risk. Not only does the MPLD identify the systems which play a role in determining plant risk, but, it also displays them in a format in way which provides an integrated visual representation or "model" of all of the elements of a PSA in a single diagram. This can be very important during the design process because it translates the basic plant design into a risk assessment tool which can be understood by the non-PSA specialist.

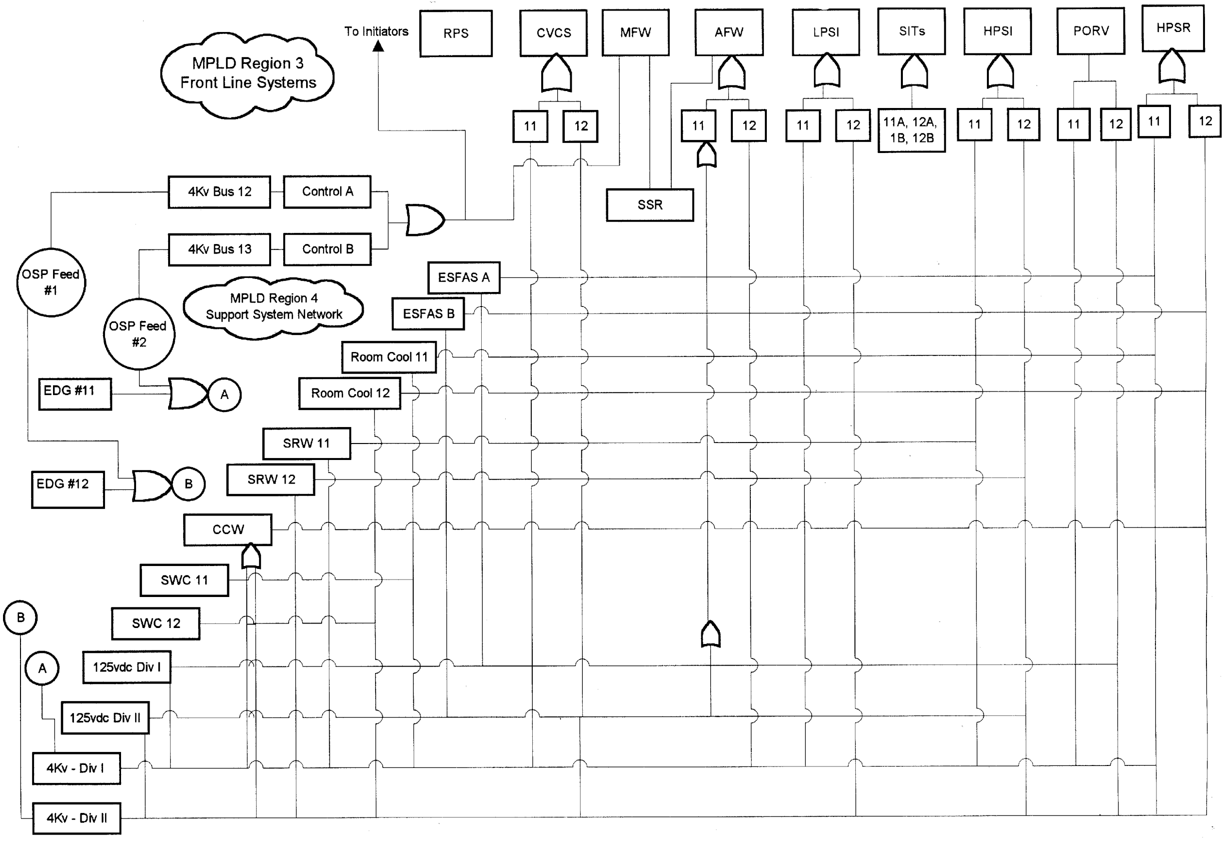


*FIG. 5-12B. Master plant logic diagram (success paths).*

The MPLD provides an explicit display of the hierarchical relationships between:

- Critical core and containment protection functions and the normally operating systems which maintain then during operation,
- Initiating events which threaten these critical functions and any associated demands for standby system operation to maintain these functions,
- Functional characteristics of front line systems, their functional success criteria and each individual front-line system success path,
- Plant support system infrastructure for both normally operating and “safety related” systems.

Completion of the MPLD provides a “cause and effect” tool which can be used to understand how individual failures can impact the need for, and availability of, success path which are needed to maintain critical plant functions. Because the model is logically coherent, it is capable of quantification.

Because the MPLD implicitly carries information about the role of all plant components which are needed during a postulated plant condition, so it is completely unrestrained in its role as an answer of the "what....if....?" questions. It is not limited to the examination of those limited set of events which are important enough to survive the truncation processes of a risk assessment.

This easy-to-use, success oriented, qualitative tool can provide the design and operational staff with an explicit display of the engineering issues associated with management of plant risks, can significantly enhance the staff's ability to cope during complex and stressful situations. Having this capability in the control room or the technical support center provides significant advantages over other, more traditional, quantitative approaches. Because the risk significance of operating plant states can be recognized quickly, and the MPLD can be used to guide the operating staff in selecting the best strategy for protecting the plant, the likelihood that the situation will get out of control will be minimized. Thus, the MPLD tool is unique in its ability to provide the basis for an effective operational safety, training and accident management programme and has attributes which are not obtainable with any other method.

Insights obtained directly from the MPLD into possible plant conditions and behavior which may lead to degraded safety can also be used to augment other plant programmes, particularly in the area of risk based operator training and accident management.

The simplified MPLD shown in Figs 5-12A and -12B was originally developed for PWR full power operation, but, has been simplified to the extent needed to be shown on a single page. This particular simplified MPLD was derived from the original PWR MPLD which was developed in 1986 for PRA methodology development. The primary simplifications to this model include:

- Removal of the containment systems,
- Coarse grouping of accident initiating events,
- Failure to show common trains, i.e. instead of showing trains A, B and AB (which is everything common to A and B, but not in scope of A or B), only A and B are shown,
- Elimination of the 480vac buses, and third safety system trains, where they exist.

A fully detailed MPLD can generally be shown in a 36" × 48" drawing, with sufficient detail to describe the entire plant reliability structure, and yet remain readable.

## Master plant logic diagram description

The master plant logic diagram(MPLD) displays the explicit interrelationships between plant critical functions, initiating events, front line systems and support systems. It has four distinct regions of interest, which are identified in Figs 5-12A and 5-12B as Regions I, II, III, and IV. The important features of each region are described below.

### Region I

Region I represents the functional plant description. The abbreviated version shows only the critical functions, but, a fully developed MPLD will identify and show the hierarchy between all important plant functions. The precise plant damage state can be inferred from the nature of the functional failure which results from each postulated accident scenario.

### Region II

There is a logical premise that core and plant protective functions must always be achieved if either,

- The plant remains in its normal operating state, i.e. no events occur to threaten normal plant critical functions or,
- All required safety systems respond successfully following an event which initiates a plant transition to an off-normal operating state.

This premise leads to the logical noding shown in Region II of the MPLD. This noding, represented by "dots" placed at the active intersects of the dependency lines which make up the network, explicitly identify which systems must respond to each specific initiating event. The logic in this display corresponds to that normally embedded in the plant risk assessment event trees.

### Region III

Region III represents a display of the "front line" or primary mitigating systems and their basic reliability structure. Each independent part of the system is shown as a discrete block, and displays its degree of redundancy. Each two train system will typically have three elements representing:

- Components in train A,
- Components in train B,
- Components common to trains A and B (note: this is not shown in the abbreviated example).

### Region IV

Region IV displays hierarchical support system network. Unless otherwise shown, the logic is "AND", and each node in the vertical represents a required dependency. Note, the MPLD is developed from the operator's perspective and shows requirements for SUCCESS rather than for failure.

### Use of the MPLD

The hierarchy of support systems allows cause/consequence analyses to be performed as shown in this example: Select a particular independent element, identified as a box in the MPLD model, and assume that it has failed. Trace the effects of this failure upwards through the dependency network and identify all consequential failures. The resulting effects on the plant critical functions, and final plant damage state can quickly be recognized.

For example, assume that 4KV bus 14 is failed. By following the dependency network in Figure 5-12B:

Loss of 4KV Div. II causes the following systems to fail saltwater loop 12, which leads to:

- Loss of one of two sources of cooling for component cooling water (CCW),
- Loss of service water (SW) loop 12,
- Loss of number 12 ECCS pump room cooling,
- HPSI pump 12, LPSI pump 12,
- (480 VAC bus 14 — not shown), which leads to failure of PORV 404.

Tracing the effects of these failures upwards through the model leads to immediate recognition of their effects on plant critical functions. The MPLD can also be used to identify the initiating events which pose the greatest threat when 4KV bus 14 has failed (LOCAs, because one entire train of ECCS and each containment energy removal system is failed.)

A similar "what...if...?" study can be done for initiating events because their effect on the support system hierarchy is also shown explicitly.

Each block in the MPLD is independent, and represents the set of components whose local failure leads to failure of the block-i.e. the block represents a set of components which are logically in series. This means that the databases for each of the MPLD blocks can be used to examine the effects or impact on plant safety from the failure of virtually any plant component. The methodological key to the success of this approach results from maintaining absolute hierarchy within the model.

The MPLD approach which restructures information normally available from a probabilistic safety assessment (PSA) and puts it in a format suitable for routine operational decision making. This graphical display shows:

- **HOW** all of the elements of a PSA relate to plant safety,
- **HOW** plant hardware and human actions relate to critical plant functions,
- **HOW** to interpret the meaning of insights and results from a PSA without the need for lengthy training or expertise with PSA methods,
- **HOW TO** answer "what... if ...?" questions to find the safety importance of plant failures.

This means that the MPLD can be used to:

- **GUIDE** the actions of the operating staff during plant operations so that plant safety is maximized,
- **TRAIN** the operating and technical support staff in accident prevention and accident management,
- **USE PSA** concepts, methods and insights to prioritize operations and maintenance activities from the control room without any complicated analyses,
- **VERIFY** that plant procedures are adequate for any postulated accident condition.

This approach provides a way for the non-specialist to use PSA techniques to make real-time risk based decisions in an operating environment.

### Model details

Initially, detailed information needed to develop the model will be incomplete, so reliance must be placed on general knowledge derived from:

- Information supplied by a specific NSSS vendor for its design (the pre-certification PSA could be a valuable source of information),
- Deterministic requirements which are imposed by cognizant regulatory authorities (redundancy, diversity and functional separation),
- Functional understanding of nuclear plant behavior,
- Industrial and utility philosophy and practices typically used in the balance of plant, NSSS systems and support system design.

The initial model is developed from the best set of information which is available. As the information quality improves, the model is modified. Where the details of the design remain undefined, "generic" information is used, i.e. its construct fidelity reflect the "most probable" design. The most important thing to consider is that lack of information is not a reason for failing to proceed with PSA development.

The results from analyses of this model are passed back to the design team who can either use them to better define their design, or to gain the necessary insights into how the design can be changed to achieve the prescribed goals at minimum cost.

Initially the model should be developed to the train, sub-system or major electrical bus level using logic which preserves all hierarchical (cause and effect) relationships.

Example:

For a two-train front line system the system hardware can be represented as follows:

(a) A set of independent front-line sub-system elements which represent
  - "Train A", "Train B", and "Train AB",
    where
  - Train "AB" represents the set of components which are neither in "A", nor in "B", but are common to "A" and "B".

(b) A dependency network which couples each plant front line and support system. Support systems dependencies will be modeled to Train A, Train B or Train AB as appropriate.

To quantify the model, failure probabilities will be developed for the trains, using "as expected" or best judgement as to their actual configuration.

### Application

The MPLD (or an equivalent integrated model) can be used by the D-RAP team qualitatively, or quantitatively, to identify:

- Risk important systems,
- Important initiating events,
- Vulnerabilities in the assumed support system infrastructure.

When location identifiers are assigned to each major functional block or functional sub-system the design team can begin to reallocate location-dependent risk contributors by imposing the effects from each important external initiator (seismic, fire, flood etc.) onto the MPLD and confirming that when all collateral damage is assumed, at least one full division of safety related equipment will remain. The advantage of having a single display of these important risk based relationships and insights which can be used to demonstrate the effects of design decisions to non-PSA specialists should not be underestimated. This graphical interpretation of the mathematical relationships between plant hardware and risk can serve a very valuable role in design, similar to that played earlier by scale construction models which served to enhance both plant constructability and maintainability, prior to the advent of CAE and CAD.

**Preliminary reference plant PSA model**

The evolution of the MPLD (or equivalent) into the preliminary reference plant model will parallel design definition and performance of the preliminary safety analyses which provide insights into the dynamic and transient behavior of plant systems and their functional requirements and required success criteria. The initial model can provide the top level logic for the PSA, and since it can be easily reviewed and changed, may justify retention and enhancement in its own right.

Initially, reference design PSA models will likely be needed for:

- Level 1 Internal events, plus internal fires and floods, for both power operation and shutdown,
- Level 1 External Events — power operation,
- Level 2 Internal Events — power operation, internal events.

The database used to quantify these models will be "plant specific" to the extent that it should be developed specifically for the plant from all appropriate data sources, i.e. each potential source of failure, repair information is screened and MTBF/MTTR data selected upon the basis of its applicability to the plant under design. In addition, it will be necessary to develop a plant specific database to describe the magnitudes and return intervals for each external hazard which is applicable to the site.

To perform the level 2 analysis it will be necessary to begin construction of the input decks for the selected deterministic codes which will be used to predict severe accident behavior and containment conditions for individually important accident scenarios. These input decks rely heavily on having correct geometric information available to characterize the behavior of the primary system, core, vessel, containment and individual compartments within containment and the plant auxiliary building which are important to severe accident behavior and fission product releases to the environment.

It may be unnecessary to perform a level 3 analysis at this stage of the design, however, if the design team needs a good documented understanding of the economic risks presented by the plant, it may be important to perform one Typically, it is possible to develop a surrogate economic model which will suffice for most decision making needs in which the questions have more concern for relative, rather than absolute values.

### 5.17.2. D-RAP applications for the preliminary reference PSA

The preliminary PSA can be expected to reflect a very good approximation to the final reliability structure for the plant, i.e. the models will mimic the logical relationships between functions, front-line and dependent systems, identify each independent plant sub-system and major SSC whose failure affects the safety of the plant, and provide preliminary containment models in which the functional dependencies between the level 1 and level 2 PSAs are explicitly included. The PSA models can retain the integration suggested by the MPLD, or, the MPLD can be used to provide the basis for event tree or fault tree development. An important difficulty in maintaining a single integrated model arises with its use to calculate frequencies. Because the models include both event frequencies and conditional failure probabilities, the PSA must use a definitive and consistent nomenclature for the event naming scheme to ensure that all important event conditionalities are maintained.

Quantification of the PSA will use a preliminary plant failure and repair database which is derived from generic industry sources to best represent the expected plant-specific hardware.

Quantification and analysis of this D-RAP PSA will provide the tools and insights needed to:

- Confirm that the plant can be expected to meet its prescribed probabilistic safety and performance goals;
- Initiate system reliability and availability goal allocations and optimization studies;
- Provides the first rank-ordered list of SSCs and insights into the character of important accident sequences;
- Provide the first insights into plant specific containment behavior and the severe accident issues which can be expected to be important to risk;
- Identify where the operators role in preventing or mitigating the effects from severe accidents is particularly important, and, use this information to begin development of the specifications for an effective plant-wide information system;
- Provide an initial basis for development of risk based technical specifications;
- Provide an understanding of the relative importance of individual SSCs and use this information to formulate the preliminary requirements for a graded QA plan and to define any specific reliability or availability specifications which may influence the selection and procurement of SSCs;
- Provide any risk-based insights and quantitative results needed to complete the preliminary plant safety analysis report and any additional siting studies or Environmental assessments which may be required;
- Provide an initial assessment of the areas in which protection from external initiating events should have a particular focus, and confirm the adequacy of the initial plant layout in maintaining sufficient physical separation between important SSCs;
- Provide an indication of the importance of shutdown events to plant risk, and identify any unique plant characteristics which may influence the selection of SSCs;
- Identify those plant areas and compartments which may be important to risk, because of the equipment they contain, and, use this information, together with an understanding of severe accident behavior, to establish initial requirements for risk based environmental qualifications for these SSCs.

### 5.17.3. Performance requirements for the PSA

Because the designers will rely heavily on the use of the PSA to provide insights into the relative merits of individually proposed design changes, it is essential that the model be capable of both speedy modification and solution. One rule of thumb, which is practically achievable, is that within 30 minutes, the PSA should be able to provide an assessment of the worth of a change in motive power for a valve which must change state on demand in a very important system, e.g. one requirement for the performance specifications for level 1 PSA performance might be that it takes no longer than 30 minutes to predict the worth (change in average CDF) of a change to a PWR in which AC motor operated valve is replaced by an air-operated, DC controlled valve in the steam supply system to an auxiliary feedwater pump.

If this requires that the baseline PSA be streamlined, it may be necessary to maintain two PSAs, which are traceable to each other and to the plant design basis. The streamlined version to answer the day-to-day design questions encountered during risk optimization, and a detailed baseline PSA to provide a complete set of detailed PSA results. The streamlined PSA will likely only be needed for level 1 internal events "at power", and perhaps "for shutdown". Typically, questions relating to other issues can be resolved by extrapolation or by a more leisurely solution of the preliminary baseline PSA.

### 5.17.4. Final reference plant PSA model

The final reference plant PSA will represent the design configuration as it goes into its commissioning or operational state. During the course of the design, as the equipment selection process proceeds and the final details of the design become defined, the PSA will be continuously updated. Ideally, the design control procedures will require the use of the PSA for all design changes so that the D-RAP PSA team:

- Remains aware of all proposed changes,
- Is able to provide insights into the risk significance of all design decisions,
- Can continuously monitor the design process and maintain parallelism between the plant design and the PSA configuration,
- Update the plant failure and repair database to correspond with the expected levels of performance from the selected equipment types and vendors,
- Provide "early warning" of potential vulnerabilities in the plant.

It is also important that the PSA team be intimately involved in the definition of the plant-wide information system so that all risk important human actions and decision making processes, either in the operation or maintenance of the plant, have an adequate information base upon which to base them. This will key into the PSA by defining the environment for operator decision making and by influencing the non-response probabilities for human actions credited in each of the PSA models (power/shutdown, internal/external events).

As a practical matter, the D-RAP team may require more than one PSA to meet its needs, although this will also depend upon the available computing power, the efficiency of the software and the nominal speed of solution for the selected PSA model structures. If the speed of solution of the baseline models is inadequate for impromptu decision making requests, a streamlined, modularized version may be needed. The speed and ease of solution for the PSA may depend upon whether it uses:

- Single Integrated (fault tree or MPLD) model,
- Large event tree/small fault tree or,
- Small event tree/large fault tree and,
- Whether the level 2 is fully integrated with the level 1 analysis, i.e. whether the level 1 output damage states become direct inputs to the level 2 analysis, or, whether the interface must be prepared separately.

If the PSA is to be used for technical specification optimization, a separate version of the level 1/2 assessment will be needed. In this version, the probabilistic contributions from test and maintenance must be removed so that the effects of SSC configuration on instantaneous risk can be used to identify important individual combinations of component, sub-system and system outages which must be prevented or controlled by plant technical specifications.

# 6. OPERATIONAL RELIABILITY ASSURANCE

## 6.1. INTRODUCTION

Section 6 of the RAP guidebook provides detailed descriptions of the important individual activities which are important to the long term success of the O-RAP. The effectiveness of O-RAP will very much depend upon the ability of the O-RAP manager to monitor all aspects of plant performance and to confirm its acceptability, i.e. confirm that the plant meets all prescribed goals, set for reliability, economy and safety. One difficulty in prescribing appropriate goals comes from the need to select goals which are both achievable and challenging. Without these attributes it is unlikely that they will continue to provide the necessary impetus for continuous improvement in the O-RAP process.

Because SSC failures which impact plant performance do so with varying degrees of frequency and severity, they introduce a second difficulty into the goal setting process, that is how to measure and compare relatively volatile short term operational average performance with the long term average benchmark goals. Turbine generator failures represent a particularly troublesome influence on measured average performance, because historical operational experience indicates that most plants will experience an extended turbine generator forced outage every ten to twenty years.

If this high consequence, low frequency, contribution to unavailability is included in the plant level goal, it allows the plant to easily meet its prescribed capacity factor goal during each year when there are no catastrophic failures of this type, and then, in the year when the failure occurs, the plant will fail to meet its goals quite miserably. This situation challenges the precept that having prescribed goals can effectively serve as an effective benchmark for the plant performance management programme, unless the goals exclude unavailability contributions of this type.

The following section of the guide explores the many issues and provides examples associated with definition and implementation of effective system and plant level performance goals for economy, safety and reliability.

## 6.2. GOALS AND PERFORMANCE CRITERIA

Initial SSC RAM goals for operation will generally be derived from the design goals set by the final reference design because they represent the plant design basis. However, these goals should be changed to reflect ever challenging, yet realistic, goals as the plant matures. These changes will compensate for permanent improvements which come from the O-RAP driven corrections to inherent weaknesses in plant design and operational management systems.

Specific performance goals for the plant and its important SSCs are needed because they provide the impetus for maintaining a continuous search for ever increasing levels of plant and SSC performance by the O-RAP team. Having specified goals, also provides the means for bringing the plant operating processes under a form of statistical control, so that the day-to-day variations in performance caused by weaknesses in plant management systems are brought under control, before decisions are made to change the process by the addition of capital improvements, i.e. to modify, replace or augment existing plant functional success paths.

This approach to plant performance management means that the search for improvement will have an initial focus on maximizing the inherent levels of performance provided by the "as built" facility, before turning to the need for hardware changes. This approach is somewhat analogous to the two-step approach statistical control processes employed in many other manufacturing or process industries, in which the process manager:

- Establishes control over the individual sub-processes and management systems until the statistical variations in primary process performance are acceptably small, i.e. fall within an acceptable range of variability, then,
- Implements changes in the process to achieve higher levels of plant performance, to the extent that it can be achieved cost effectively.

The following suggested approach appears to represent one of the most promising practical alternatives which are open to use in the operational SSC goal setting process. This approach is promising, not only because it brings the successfully tested precepts of "statistical process control" into the nuclear plant management process, but also because it implicitly corrects for the aberrations in performance discussed in Section 6.1 above. The specific steps in the goal setting approach are as follows:

- Establish baseline SSC goals from the system level models developed for the RAM and PSA analyses for the final reference plant design, i.e. initially, equate each SSC reliability and availability goal to its calculated, or predicted, value.

Note:
These goals contain actuarially derived unavailability and unreliability contributions from all causes.

- Monitor the performance of all SSCs during plant operation and identify each individual contribution to unavailability and unreliability and its associated causes review the identified causes for each observed SSC failure and establish whether the failure was "maintenance preventable", i.e. whether a maintenance action could have been taken, "a priori", to prevent the particular event,
- Identify the percentage contributions to unreliability and unavailability from "maintenance preventable" failures, and remove them from the goals, i.e. increase the reliability and availability targets to level which exclude all expected contributions from maintenance preventable failures,
- Continue the process of incrementally increasing the goals until they compensate for all sources of preventable loss, and establish them as the bases for further performance comparisons.

If the above suggested approach were used to establish targets for the performance levels of individual SSCs during the early years of plant life, any future observed variability from these goals should serve as a performance indicators which reflect the effects from either weaknesses in management systems which remain uncorrected and result in repetitive failures, or, indicate the presence of new problems, perhaps resulting from the effects of plant ageing.

These management system weaknesses must not only be identified, but, also corrected, if their trends are to be useful as SSC performance indicators which can be used throughout the plant safety, reliability and economy improvement process. The need to focus on management systems to achieve continuous improvement adds even more emphasis to the importance of ensuring that the routine application of an effective root cause analysis (RCA) programme is an integral part of all plant performance improvement programmes and that RCA is extremely important to the success of the O-RA programme.

## 6.3. O-RAP MANAGEMENT PROCESS

### 6.3.1. Risk and safety based decision making

The use of performance monitoring and the insights it provides to guide the plant decision making process is at the heart of O-RAP and provides an integrated platform for the optimization of plant economic performance and safety.

*6.3.1.1. Risk based plant management*

The generic requirements for a plant-wide risk-based management process can be satisfied by a programme which meets the following requirements:

- The facility management has access to risk assessment models which provide a complete description of the plant risk profile, while keeping in mind their limitations and boundaries,
- The available risk models must be capable of modification to reflect both proposed and actual changes to:
  (i) Plant state or operating configuration,
  (ii) Performance levels or capabilities of individual systems and components, and,
  (iii) Human interfaces,
- The modified models must be capable of re-solution to find the new plant risk profile, and that the timeliness of the re-solution is consistent with the needs of the decision making process,
- The O-RAP team has the ability to identify and measure institutional effects which influence the effectiveness of the human as he interacts with the hardware, and incorporate the more important effects into the plant risk models. These effects are typically measured as:
  (i) Changes in the likelihood for humans acting in the role of configuration or systems operations managers will make errors and,
  (ii) Changes in the availability/reliability/maintainability of individual components,
  (iii) Sub-systems or systems which are attributable to imperfectly performed maintainer/maintenance actions.
- The O-RAP team can predict or measure the effects of the calculated or assessed changes in plant risk in terms of performance measures or metrics which are consistent with operating/management personnel experience.

The risk assessment models mentioned above are sufficient for facility management to use to establish "the worth of a change" and make technically justified decisions as to the disposition of proposed or needed changes. However, the PSA does not intimate how the change is to be effected. This means that there are always two parts to a comprehensive risk-based management programme:

(a) Identification of areas in which change is needed, and quantitative assessment of the individual worth of all proposed changes,
(b) Identification of ways in which the needed change can physically be achieved.

Conventional PSAs achieve only the former, and do so only on the basis of the assumptions made during the analysis regarding:

(a) Component unavailabilities (data and its processing),
(b) Component/system functional requirements and capabilities (event sequences and success criteria) and,
(c) Points and degree of human interactions (human reliability assessment and plant behavior).

*6.3.1.2. PSA applications*

Applications for the analytical models and their associated solution methods in the overall plant management process are broad, so the following summary of potential applications has been developed to provide the general framework within which their power and capabilities can be appreciated.

6.3.1.2.1. Decision making with a "living PSA plant model"

A completed PSA provides a "snapshot" in time of the plant's risk profile and reliability characteristics. Maintaining a living PSA requires that all changes to the plant be evaluated and, when applicable, incorporated into the PSA, since any change in the plant procedures and/or hardware has the potential to change the plant's characteristics and the PSA results. The living PSA provides a current model which can be used to quickly evaluate the absolute and relative merits of potential changes or alternative operational strategies.

The “fast solver” PSA, which has been updated to match existing plant configuration, i.e. reflects modifications and institutional and organizational changes which have been implemented to that point in the life of the plant, serves as an effective engineering tool which can guide the justification and prioritization process for all proposed future changes and confirm that the plant continues to meet all assigned probabilistic safety criteria.

In addition, because decisions on scheduling equipment outages can benefit from an examination of their associated impacts on risk, the living PSA can be a very useful analytical tool which can be used by plant maintenance planners.

For example:

If auxiliary feedwater pump A is currently "out of service" for repair, and the incremental risk associated with taking DC bus B down for a particular maintenance activity at the same time, is unacceptably large:

- maintenance on the DC bus should probably be delayed until the plant is in a less sensitive configuration,
- The operators should be told of the "alert status" associated with the particular configuration, together with the conditionally important "dominant risk sequences". This would allow them to plan and implement compensatory measures which will reduce the magnitude of the associated risk exposure,
- If the DC bus requires maintenance which cannot be delayed, the operations staff should have approved contingency plans in place.

Use of a PSA to manage configuration risk in near real time, will require the use of a special, very fast solving PSA model in which the contributions from unavailability due to maintenance have been removed.

#### 6.3.1.2.2. "Risk-based inspection and testing" programme

Inspection and test programmes are designed to examine passive components to detect any signs of deterioration of their capability and to test standby components to ensure their operability. Optimum scheduling of inspection and test intervals should be based upon the risk significance of potential failures of the components and upon the expected time interval between the appearance of early failure symptoms and the time at which the component will fail.

#### 6.3.1.2.3. Applications involving hardware replacement

Having RAM and PSA models for individual plant systems which can provide quantitative relationships between SSC performance, system availability, plant availability and public health and safety will facilitate the plant RAP staff's ability to identify areas in which proposed improvements to the reliability, availability or capability of the hardware or human may be particularly valuable.

Manipulation of these models will also allow them to predict the economic value or other benefits which may accrue from any proposed changes to the plant or its man-machine interface. Cost/benefit studies can be readily performed to provide a rational and technically sound basis for future decisions.

Initially, when there is little or no plant operating experience, generic information taken from a multi-industry data bank provide the basis for expected levels of SSC performance. As the plant matures and increasing amounts of plant-specific failure and repair data become available, the generic data can be adjusted to reflect this plant-specific operating experience. In addition to updating or adjusting the plant SSC database, the plant models will also be updated to ensure that they match the current plant configuration and institutional character.

A suite of plant specific risk models which are easily solved within the time scales important to each type of plant decision can provide the O-RAP team with very effective decision making resources. The following limited set of potential applications are provided to exemplify the range of possible applications for a PSA which can be exploited in individual O-RAP elements. The primary uses for RAM and PSA modeling capabilities are associated with the estimation of the individual "worth" of proposed changes so that their cost effectiveness can be estimated.

#### 6.3.1.2.4. Potential PSA applications for plant engineering

Examples of the several different and complementary ways in which PSAs are able to assist in the plant performance based management processes are described by the following:

*Baseline risk profile, vulnerability assessment and ranking SSCs:*

The baseline assessment is used to identify the "as designed" or "as built" plant risk levels and to provide a list of the individual contributors, ranked in order of their importance to risk and safety.

This ranked list of contributors becomes the starting point for a comprehensive risk reduction programme whether in the design stage or post-construction. The most important individual SSCs are those which are likely to provide the opportunities for the implementation of cost effective improvements

*Condition monitoring analysis:*

The process of gathering information "on-line" for operating or standby hardware to provide an inference of internal condition or proper alignment can lead to real time assessments of failure propensities.

The net benefit of these systems can be assessed with a risk model so that an estimate of their effectiveness can be established and the decision to install them made on a cost-justified basis.

*Integrated living schedule (ILS) or integrated management system (IMS):*

ILS/IMS is a process by which the implementation schedule for proposed facility changes is optimized on the basis of risk, within the normally present schedule and budgetary constraints.

The PSA can provide the necessary insights to ensure the effectiveness of the programme by providing insights into the relative risk significance of each of the items in the schedule, and ensuring that the prioritization process always guides the plant maintenance planning staff in implementing the most risk significant plant enhancements first.

*Life cycle costing*:

This is the process of allocating resources for facility improvements on the basis of their impact on lifetime facility costs. The PSA models provide a mechanism for simulating the worth of the changes during the expected plant lifetime so that their integrated benefits can be estimated, and compared with the costs of their implementation.

*Man-machine interface enhancement:*

The role of the human is critical in the operation of all industrial and nuclear facilities. Solution and quantification of the plant risk model can provide a rank ordered list of human actions whose successful interface with the plant hardware systems are particularly important to the plant during both normal, and off-normal conditions.

This same capability can also be used to establish "worth" of changes to this interface and by examining how changes in the information presented to the operating staff can affect the likelihood of success the O-RAP team can ensure that resources expended to improve them are expended in an optimal manner.

*On-line process disturbance analysis and intelligent monitoring and alarming:*

Monitoring system parameters on-line may identify changes which are precursors to more significant events. A fault is diagnosed and provides forewarning to the operator so that preventive measures can be taken in time to mitigate an event which may become an "initiator".

This type of system can also be used to diagnose system state during an upset so that direct event-specific recovery actions can be implemented by the operating staff, and limit the severity of the event. The cost effectiveness of the system can be established with the risk models.

*System interactions:*

The safety characteristics of a facility are often dominated by interactions between two or more seemingly independent systems. A risk assessment can identify coupling mechanisms and can provide a quantitative assessment of their importance. The assessment can then be used to evaluate the various proposed countermeasures and allow the identification of the most appropriate response.

#### *6.3.1.3. Risk based applications for plant operations*

The availability of models of the plant systems and knowledge of how operational procedures and maintenance policies affect system availability, plant availability, and public health and safety makes it easy and economical to do thorough studies of the implications of any proposed changes to the procedures and policies.

*Administrative policies/practices evaluation:*

Administrative policies/practices evaluation is a process by which the effects of proposed changes to the management and operation of a facility can be measured in terms of their impact on hardware and human performance, and their "worth" established a priori with a risk model.

*Performance analysis:*

Performance analysis is the process by which the individual events which occur in the operation of a facility can be simulated in the risk models to provide a high-level indication of facility performance. Performance indicators can be identified as surrogates for these detailed assessments.

*Risk-based inspection and testing programmes:*

A probabilistic risk assessment of a plant provides a basis for the prioritization of systems and components in terms of their risk importance. This can provide a rational basis for the scheduling of inspection and testing of those components and systems.

*Risk importance of operating events:*

To ensure that requisite resources are applied in the prevention of events which have risk significance, a risk assessment can provide direct estimates of the actual risk exposure from an experienced event. The magnitude of risk exposure for experienced events can then be used to prioritize the allocation of resources for a Corrective Actions programme.

*Technical specification conformance and optimization:*

The technical specifications are designed to maintain the validity of the assumptions made in the facility safety analysis. It is economically important that they be no more restrictive than necessary, so risk assessments can be used to relax the requirements where appropriate. The duration of allowed safety equipment outage times and the frequency of required testings are defined by the technical specifications. These can be optimized with a risk assessment by ensuring that the requirements are modified to maximize the availability of individual hardware systems while maintaining an acceptably low level of risk.

#### *6.3.1.4. Additional applications*

A facility risk assessment provides a valuable resource-the list of dominant risk contributors. This list of those scenarios or event sequences which contribute most of the facility risk allows one to carry out accident planning in an effective manner so as to ensure that personnel are prepared to deal with the most important classes of off-normal operation.

*Accident management:*

Risk assessments provide a clear definition of the dominant facility accident scenarios and can be used to develop strategies for dealing with accidents (planning) and in some cases can be used during an accident to prioritize the operator's recovery and mitigation actions.

*Risk informed focus for training programme*:

A baseline risk model allows the plant training programme to develop effective procedural responses for the important scenarios identified by the risk analysis, and to allow prioritization within the training programme to ensure that the programme recognizes all the dominant risk contributors.

The PSA programme can also be particularly valuable in the operator simulator training programmes because the plant staff is well practiced in their management of each important high risk and high frequency accident scenario, plant risk can be reduced significantly. This is not to imply that only the high frequency, high risk scenarios are practiced, but, that as a minimum they should all be part of the operator training programme.

*Emergency drills:*

For the same reasons that an expert understanding of the plant risk profile is important to the operator training programme, it is also important to the emergency preparedness programme, for many of the same reasons. The programme should try to base the periodically performed emergency drills on real, risk-important scenarios so that all participants have practice in responding to those scenarios which the plant PSA indicates are important.

However, because the emergency drills attempt to provide practice with many response programme elements which may not necessarily be part of the selected PSA scenario, they may require modification to meet specific emergency planning programme needs.

*Emergency planning zone definition:*

The results from the baseline level 3 PSA can be used to identify an appropriate plant emergency planning zone (EPZ) which will ensure optimal preparations for protection of the general public, following a release of fission products, by evacuation, sheltering and the use of blocking agents. These preparations may include development of a warning system (sirens) and preplanning of emergency protective actions which must be taken by plant and public emergency response teams within the area bounded by the EPZ.
Because there is a significant life-cycle cost associated with maintaining an effective emergency planning programme, if the affected EPZ can be reduced to its risk based optimum, a potential exists for significant life time cost savings.

*Land use planning:*

Though the land use issue surrounding a nuclear power plant may often be beyond the purview of the plant operator/owner, it is an important issue. Related to the maintenance of an effective, yet optimal emergency planning zone, is the use of the PSA results and insights to manage land use around the plant and prevent any unexpected or unplanned changes in local demography and population mobility which could increase risk to a point that it is unacceptable to society.

### 6.3.2. Management of reliability, availability and maintainability improvement programmes

#### *6.3.2.1. Root cause analysis*

Before an improvement in the availability or reliability of a specific component can be achieved, the reasons for its actual operational performance must be clearly identified. It is not until existing component behavior is understood and likely hypotheses for the causes of its unavailability synthesized, that strategies for improvement can be formulated and initiated. Improvements in component availability can result from either a reduction in its failure frequency, or the restoration time which follows a failure. The relative importance of each contribution depends upon the specific situation. The important thing is that the availability engineer actively considers both elements during the improvement process.

The above implies that there are two elements of a root cause analysis which are important to component availability improvement:

- Confirmation of hypotheses which describe the reasons for failure, or unreliability;
- Identification of the reasons for time expended during the repair, or causes of unmaintainability.

When the availability engineer has the reasons for both contributors to component unavailability, strategies for improvement can be formulated.

#### 6.3.2.1.1. Definitions for root cause

The definitions for root cause may vary from user to user, but, their meaning is generally the same, i.e.

- The root cause(s) for a particular failure event can be defined as the underlying or prime reason(s) for its occurrence, which if prevented from occurring again, will also prevent recurrence of the experienced, or similar, failure events;
- The root causes for a particular failure will **invariably** involve the failure of a management system.

*Multiple or single root causes:*

Since multiple failures are often necessary before a functionally important damage state is reached, **multiple** root causes will be invariably implicated in the functional failure of a critical SSC.

#### 6.3.2.1.2. Objectives for root cause investigation

The root cause investigation has several major objectives, i.e. to:

Identify what actually happened, i.e. the sequence of events which led up to the observed failure;

Identify the critical events, i.e. those failure events, which had they been prevented, would also have prevented the observed failure under investigation;

Identify root causes, i.e. the causes, generally management system failures, that led to the occurrence of each critical event in the failure scenario.

#### 6.3.2.1.3. Root cause analysis — functional steps

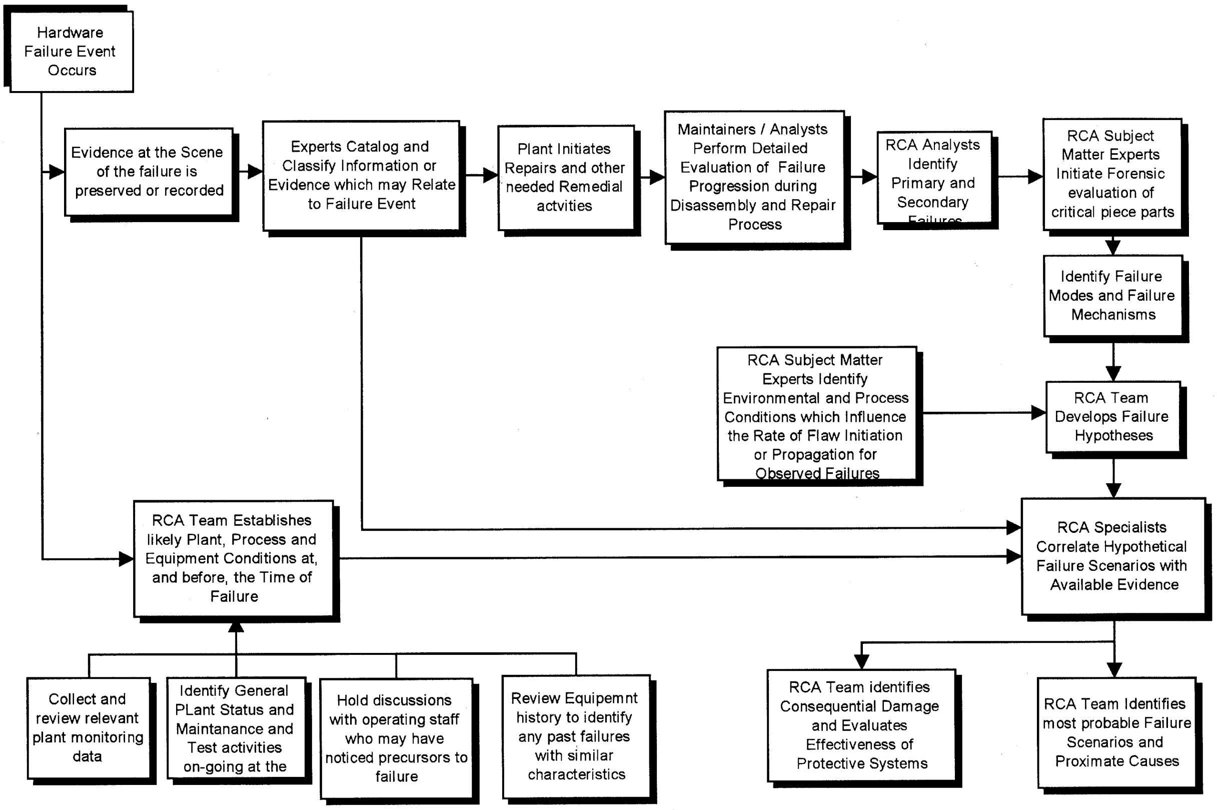
There are several fundamental steps which are common to all root cause investigations. These steps typically include:

- Collection and analysis of information to identify the specific conditions prevailing at the time of the failure, and any evidence which can be used to confirm the presence of specific failure modes or mechanisms. Placing the information in chronological order is generally a good first step in analysing the information and sorting out facts, conditions and identifying critical events;
- Formulation of hypothetical scenarios and the sequence of events which may have occurred before, during and after the failure. Sometimes, deductive (goal or fault trees) or inductive (FMWEA or event trees) models are developed to aid in their identification;
- Correlation of the available information with that expected during the hypothesized scenarios and identification of those which most likely represent actual failure scenarios;
- Confirmation and or refutation of specific failure scenarios to find the initiating causes;
- Determination of specific reasons for the failure and identification of cost effective remedial actions which minimize the future impact of like failures.

The root cause investigation process shown in Figures 6-1 and 6-2 and described below represents a general approach and philosophy. Each element in the process does not necessarily have to be followed in sequence and the way in which the process is used for a specific investigation may depend very much upon how much information is know from the outset. The information gathering can be done in parallel with scenario development, if the likely scenarios can be defined from general information available to the investigators at the time of the failure.

Immediately following the occurrence of a failure it is essential that any evidence which may shed light on the reasons or the sequence of events be preserved to the maximum extent that is practical and justified by the importance of the failure. This means that the investigatory team should be called in immediately and initiation of equipment repairs delayed until this evidence has been catalogued. The number of personnel who have access to the equipment should be limited until this task is complete. The evidence and information which should be sought (depending on the type of the failure) should typically include:

- Location of pieces which may have broken away — this can provide information on the direction and energy release during any catastrophic failure;
- Identification of any lubricating or cooling fluids which may have been leaking prior to the failure, and their locations relative to the hardware;



Hardware Failure Event Occurs
Evidence at the Scene of the failure is preserved or recorded
Experts Catalog and Classify Information or Evidence which may Relate to Failure Event
Plant Initiates Repairs and other needed Remedial actvities
Maintainers / Analysts Perform Detailed Evaluation of Failure Progression during Disassembly and Repair Process
RCA Analysts Identify Primary and Secondary Failures
RCA Subject Matter Experts Initiate Forensic evaluation of critical piece parts
Identify Failure Modes and Failure Mechanisms
RCA Subject Matter Experts Identify Environmental and Process Conditions which Influence the Rate of Flaw Initiation or Propagation for Observed Failures
RCA Team Develops Failure Hypotheses
RCA Team Establishes likely Plant, Process and Equipment Conditions at, and before, the Time of Failure
RCA Specialists Correlate Hypothetical Failure Scenarios with Available Evidence
Collect and review relevant plant monitoring data
Identify General PLant Status and Maintanance and Test activities on-going at the
Hold discussions with operating staff who may have noticed precursors to failure
Review Equipemnt history to identify any past failures with similar characteristics
RCA Team identifies Consequential Damage and Evaluates Effectiveness of Protective Systems
RCA Team Identifies most probable Failure Scenarios and Proximate Causes

*FIG. 6-1. Root cause analysis — identifying the failure scenario.*

*RCA element 1 — preservation of evidence*

- Integrity and operability of support systems which maintain operation of the hardware such as cracked instrument control lines, electrical or control connections, auxiliary pumps, heat exchangers, filters, etc.;
- Checking the "as found" position or condition for all manual and control valves, breakers, relays, couplings, fuses;
- Checking for evidence of severe heating, arcing or corrosive degradation on the component or any of its auxiliaries.

All of the information should be catalogues and if possible photographed or videotaped (in true colour) to provide documentary evidence for the investigatory team to go return to later on.

*RCA element 2 — detailed evaluation during repair*

A great deal of important information can be obtained from a careful examination of the hardware during its disassembly for repair or refurbishment. Of importance might be:

- The actual location of any damaged or broken pieces or foreign bodies;
- Any pattern or location of distortion, misalignment, wastage or erosion, or overheating of parts;
- Whether at the onset of repair, rotating equipment is free to rotate, or, is seized;
- Whether there is evidence of excessive wear, play or motion;
- Documented evidence of unusual or unexpected material coatings which could be removed during normal handling:
  - Grease, oil or water in unusual places,
  - Carbon from arcing or burning,
  - Corrosion products,
  - Chemical deposits or dirt.

The information gathering process described above is comprehensive. In some cases, past experience can allow shortcuts because before the work begins the analyst may know the likely causes. Even so, collection of the evidence, both circumstantial and hardware failure specific must be rigorous and consistent.

*RCA element 3 — establishing conditions at the time of the failure*

It is rare that failures occur without the emission of some prior indications or precursor information. Frequently, however, unless someone specifically is charged with looking for it, the information is overlooked. The goal of the RCA investigator is to go back in time, find this information and correlate it with the failure event to confirm or refute any postulated failure hypotheses. This circumstantial evidence may be short term, i.e. immediately preceding the failure, or may be long term and include anecdotal information from earlier failures or from previous operating experience. Resources which can be utilized by the RCA analyst include:

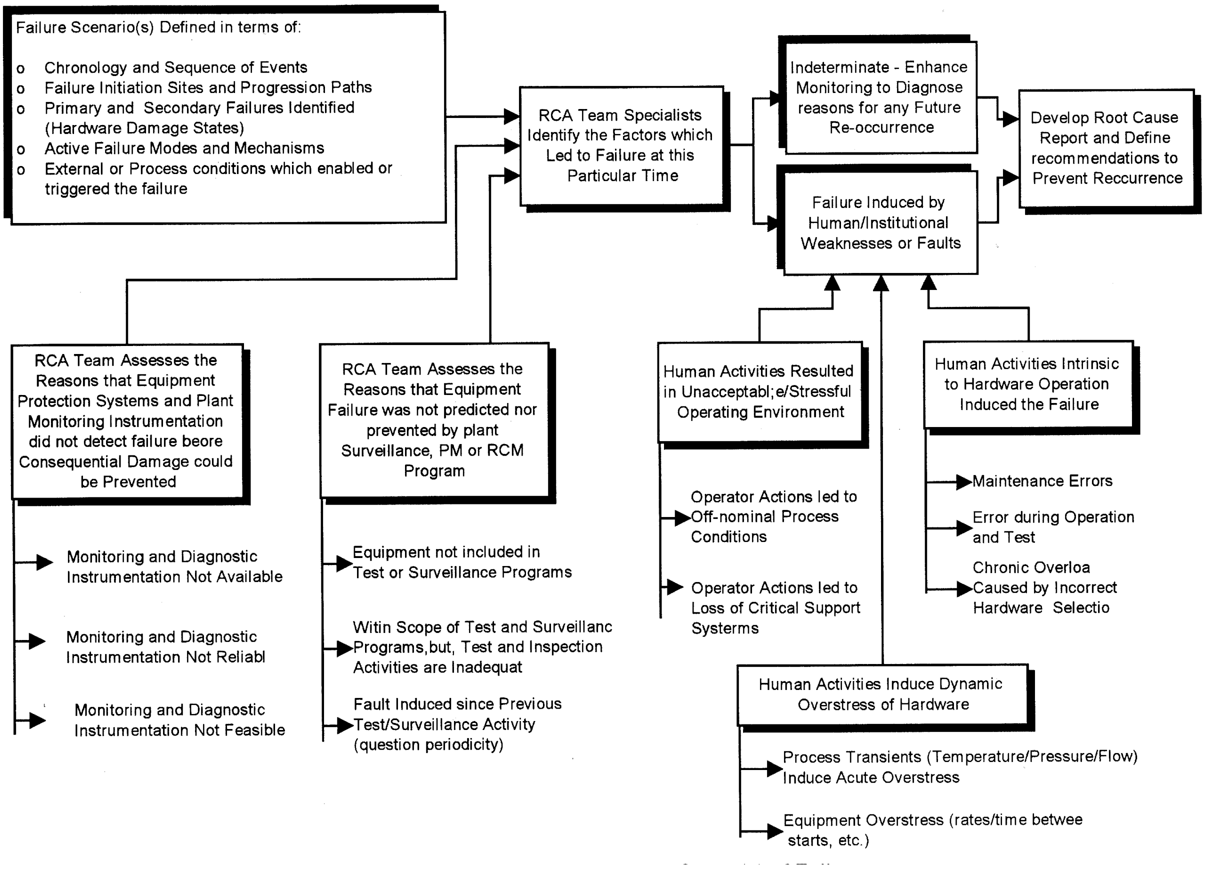

Failure Scenario(s) Defined in terms of:
o Chronology and Sequence of Events
o Failure Initiation Sites and Progression Paths
o Primary and Secondary Failures Identified (Hardware Damage States)
o Active Failure Modes and Mechanisms
o External or Process conditions which enabled or triggered the failure
RCA Team Specialists Identify the Factors which Led to Failure at this Particular Time
Indeterminate - Enhance Monitoring to Diagnose reasons for any Future Re-occurrence
Failure Induced by Human/Institutional Weaknesses or Faults
Develop Root Cause Report and Define recommendations to Prevent Reccurrence
RCA Team Assesses the Reasons that Equipment Protection Systems and Plant Monitoring Instrumentation did not detect failure beore Consequential Damage could be Prevented
Monitoring and Diagnostic Instrumentation Not Available
Monitoring and Diagnostic Instrumentation Not Reliabl
Monitoring and Diagnostic Instrumentation Not Feasible
RCA Team Assesses the Reasons that Equipment Failure was not predicted nor prevented by plant Surveillance, PM or RCM Program
Equipment not included in Test or Surveillance Programs
Witin Scope of Test and Surveillanc Programs,but, Test and Inspection Activities are Inadequat
Fault Induced since Previous Test/Surveillance Activity (question periodicity)
Human Activities Resulted in Unacceptabl;e/Stressful Operating Environment
Operator Actions led to Off-nominal Process Conditions
Operator Actions led to Loss of Critical Support Systerms
Human Activities Intrinsic to Hardware Operation Induced the Failure
Maintenance Errors
Error during Operation and Test
Chronic Overloa Caused by Incorrect Hardware Selectio
Human Activities Induce Dynamic Overstress of Hardware
Process Transients (Temperature/Pressure/Flow) Induce Acute Overstress
Equipment Overstress (rates/time betwee starts, etc.)

*FIG. 6-2. Root cause analysis — identifying the cause(s) of failure.*

Plant status:

- Control room or operating logs sheets or power history plots showing the plant state prior to the failure;
- Activities associated with the system in which the failure occurred such as equipment being started or shutdown;
- Maintenance logs which define the extent of maintenance or testing activities going on.

Plant monitoring:

- Parameter traces or trend data which show the system or process conditions prior to the failure;
- Any condition monitoring information which is maintained or taken on a continuous or periodic basis — vibration, temperature, pressure, flow, fluid levels, etc.

Plant history:

- Correlation between earlier failures and plant status or operating capability;
- Past experience with similar failures and any information relating to their possible causes;
- Relative timing between failures and specific maintenance or testing activities;
- Relative timing between experienced failures and specific plant evolutions.

Operators and maintainers:

- Evidence for anomalous behaviour, such as noise, vibration, temperature, degraded capability or unusual environmental conditions (heat, cold);
- Need for operational maintenance, such as filling oil reservoirs, adjusting cooling water flows, cleaning heat exchangers, adjusting controls;
- Any observable trends or information which may, in retrospect, have been indicative of long term degradation or changes in equipment behaviour;
- Any previous operational occurrences which, at the time caused no problems, but could possibly have stressed the component — too many starts on a motor, too fast a startup on a turbine, high vibration on an earlier start, etc.

All of this information, typically collected or elicited by skilled and trained interviewers or from review or relevant plant documents should be recorded in a consistent, accessible and easily processed format.

*RCA element 4 — forensic analysis and evaluation*

Each of the damaged parts removed from the damaged or failed equipment should be subjected to a detailed forensic analysis to determine the exact cause of failure. Failure of a piece part only occurs when it is subjected to a load, dynamic or chronic, which exceeds its. strength.

This important insight provides the forensic analyst with the requisite foundation for his analysis. He must look specifically for evidence which provides both the initiation site for the failure and its progression path, and the preexisting conditions which led to the initiation.

Strength of the piece part is affected by:

- Material properties — elasticity, ultimate strength, toughness, ductility, fatigue strength, etc.;
- Material integrity — presence of flaws, cracks, inclusions, pits, etc.;
- Material dimensions — presence of wear, creep, erosion, corrosion, thinning, etc.

Loads on the piece parts can be chronic, dynamic and cyclic and can result from:

- Cyclic: vibration from rotating imbalance, misalignment, process induced flow and pressure vibration, shock, varying thermal gradients, slug flow;
- Dynamic: impacts from rubs, contacts between rotating/reciprocating/stationary piece parts:
    - severe dynamic pressure differentials, high torque loads from locked rotor events,
    - feedback from external loads;
- Chronic: continuous overspeed, excessive power (beyond design nominal), thermal stress, structural bending loads, etc.

Having an understanding of a fundamental failure philosophy, typified by the examples above, the forensic analyst must seek evidence which shows or confirms the actual failure mechanism. He will perform analyses to confirm material properties, examine the actual failure sites to identify the nature of the failure, fatigue, stress corrosion cracking, intergranular stress corrosion, embrittlement, etc.

To this point in the analysis all the pieces are in place to provide confirmation or refutation of the failure hypotheses. In reality, for many failures, general knowledge of component failure behaviour used in combination with the information gathered would have provided the foundation for a diagnosis of the cause of failure and the definition of the failure scenario. In the case of insidious or very complex failures or in the case where little or no information is available, this may not necessarily be the case, and detailed potential scenarios must be constructed to provide some directions to the analyst's thoughts.

The development of scenarios can be done with a predefined model, or can be constructed in "event tree" format. The goal of this task is to identify likely initiating failure events and be able to follow their progression to the experienced damage state. Look at each scenario, identify the evidence that would be available if it were the actual scenario, and compare this with the observations.

A match then indicates the scenario which actually occurred, so at that point the cause of the failure is identified. I a match cannot be made, a search for more information via enhanced monitoring or whatever other practical means can be employed is planned so that in the future confirmation can be made.

*Event causation and management system failures*

To this point, the process has identified the actual sequence of events which occurred. The next task is one of identifying why the failure occurred. It isn't until the "why" is truly answered that all corrective or remedial actions can be employed.

When an unexpected failure occurs, and presumably it will be unexpected if a root cause investigation is proposed, it is because either something changed while the component was operating and a stress was imposed on the component (increased load) or the strength of the component was degraded but had been undetected. The questions to be answered then become focused on plant management systems and why:

- Plant surveillance, test or inspection programs failed to detect the incipient failure;
- Plant preventive maintenance or reliability centred maintenance programs failed to prevent the failure;
- A human error led to the failure:
    - Maintainer errors which rendered the SSC unavailable when needed,
        - not restored to full operability following an earlier maintenance, test or inspection activity, i.e. valves closed, actuation or protective systems not reconnected, cooling systems unrestored, lubrication systems inoperable (blind orifices in lube oil lines, low oil levels), control systems or set points out of calibration;
    - Maintainer errors which reduced the reliability of the SCC,
        - loose bolting, misaligned shafts and bearings, gaskets not sealed, internal clearances incorrect, foreign materials left in the component or system, etc.;
    - Operator errors which led to a system transient and caused the failure,
        - closed pump bypass lines, sudden opening of bypass lines, over-pressurization, dynamic instability, operating a pump with reduced flow, running a pump out on its curve. Some of these events could result indirectly from improper bypass of equipment protection trips or isolation of monitoring devices;
    - Operator errors associated with improper valve line-ups or isolation or needed component auxiliary systems.

All of these failures show how human failures are potentially involved in all failure scenarios, and why the human side must be explored to really find out "why" each critical event in a failure scenario occurred. This leads to the investigatory themes shown in Figure 6-2, i.e.

- Why the failure was not predicted or prevented by plant programs (if not caused directly by a human error);
- Why the human acted in error if it was the direct cause of equipment failure.

It is not until both of these questions have been answered, that effective corrective actions can be instituted to prevent recurrence. Because the high importance of "maintenance preventable" failures in setting SSC performance goals and in establishing "statistical process control" over plant management systems and processes, the root cause analysis program must be specifically geared to, as a minimum, identifying the reasons for these types of contributing fault events.

*RCA element 5 — reporting and recommendations*

When the investigation is complete and validity of the hypotheses relating proposed root causes to the observed event has been confirmed with the available evidence, the RCA team must detail its findings and identify recommendations which will be effective in preventing their recurrence.

The recommendations should be:

- Clear, unambiguous, address management systems weaknesses and fix the problem;
- Specific, feasible, practical and cost effective;
- Clear in defining the requirements for implementation.

The identified root causes should also be communicated to all plant staff who are involved in similar activities so that they are aware of the reasons for the failure and can ensure that analogous conditions are removed before they also lead to similar failures elsewhere.

There are many individual management programs, systems and processes which are implemented to achieve specific O-RAP objectives. This section of the guideline describes some of the individual activities which are particularly important to the management and assurance of operating plant reliability, availability, maintainability and economy.

#### *6.3.2.2. Reliability centered maintenance*

Prevention of repetitive, maintenance preventable, hardware failures is one of the most important programmatic objectives for an O-RAP. When a comprehensive Reliability centered maintenance (RCM) program is implemented in concert with other )-RA programs, it can be effective in providing key programmatic attributes which leads to the achievement of this particular objective.

The premise within this statement lies with a realization that the contribution to plant or safety system unavailability from maintenance preventable failures can be minimized if:

- The effectiveness of the content and periodicity of each individual SSC preventive maintenance activity is maximized so that the expected number of unplanned SSC failures is minimized;

- The causes for each failure are determined so that maintenance preventable failures can clearly be recognized and corrected, wherever they contribute to SSC unreliability or unavailability;
- Enhanced planning and preparation is implemented for all SSC maintenance activities.
- This means that maintainers are fully prepared for each activity, i.e. trained in the use of the necessary procedures and practices, so that they are placed in as few error prone situations as possible, and exhibit minimal error rates for individual maintenance activities which influence SSC reliability and availability.

A reliability centered maintenance (RCM) program, coupled with an effective root cause analysis (RCA) capability can provide the necessary foundations for this O-RAP activity. reliability centered maintenance is a proven technique for formulating a preventive maintenance (PM) program or improving an existing PM program.

Instead of placing reliance on vendor recommendations for individual components, RCM uses a system function based approach to identify the important functional failure modes, their potential causes, the then identifies maintenance activities which prevent, or minimize the likelihood, that they will occur.

RCM seeks to identify:

- The important functions of each system in the plant;
- Those component failures which impact system function;
- Applicable and effective maintenance actions.

By following this formal regimen of hierarchical tasks, the program focuses on the prevention of those failures which have the greatest impact, i.e. have the greatest importance to safety or economy.

During the process of identifying the preventive maintenance actions which prevent unplanned failures, the RCM process deliberately attempts to maximize the use of "on-condition" and predictive maintenance tasks instead of more traditional "time directed" overhaul tasks. It is this particular attribute which tends to result in an overall reduction in the number of maintenance actions performed for a particular SSC.

Another important attribute of the RCM process is that the RCM process identified the individual SSC functional failure modes of concern and identified specific maintenance tasks which can be initiated to either prevent, or reduce their occurrence frequency. Not only does the program move preventive maintenance programs away from the traditional use of routine periodic overhauls, but, also focuses attention on the implementation of maintenance activities which fix know or suspected, actions which can be well planned in advance.

When the RCM process is coupled with an effective root cause investigation program, whose primary focus is on determination of the reasons for each unplanned failure by asking the specific question, "why didn't the RCM program prevent the unplanned functional failure", all maintenance preventable failures should be identifiable, together with their associated causative weaknesses in plant management. This information can facilitate the "continuous improvement process" throughout the life of the plant within the framework of a "living" RCM program.

*Typical RCM process*

The overall RCM process is described in Figure 6-3 and the following functional descriptions of specific activities which are part of every RCM program:

- Collect system related information and any existing preventive/corrective maintenance data which may indicate which systems or SSCs should be included in the program;
- Explicitly define each system boundary, sub-system and component functions, their functional interfaces with other systems and important sub-system and component functional failures and failure modes;
- Perform a detailed functional review of each system, infer the plant level effects from each individual SSC functional failure and perform FMEAs to identify the dominant functional failure modes for important SSCs;
- Use qualitative and quantitative reliability modelling and analysis techniques (FMEAs, FTAs, GTAs) to identify the relative importance of individual SSCs;
- Identify an effective maintenance strategy which prevents the occurrence of these important failure modes and prevent unplanned functional failures of important SSCs. Options which should be considered will include:
    - Condition directed corrective maintenance tasks, initiated upon detection of unacceptably degraded internal SSC conditions which are inferred from an external monitoring and diagnostic process;
    - Implementation of a formal fault finding process for important SSCs which identified incipient faults and triggers the initiation of an appropriate corrective maintenance strategy;
    - Time directed maintenance tasks whose periodicity is derived from an understanding of the SSC failure modes, their rates of progression and their impacts on SSC reliability;
    - Correction and refurbishment after functional failure, i.e. make no attempts to implement a preventive maintenance strategy. This approach is sometimes referred to as “running to failure”;
- Identify specific maintenance actions which will prevent the occurrence of each important failure mode, discovered under one of the four conditions described above;
- Determine an appropriate inspection or overhaul interval for each SSC whose selected strategy does not involve continuous monitoring or maintenance on condition;
- Document the basis for the PM program so that as future changes or enhancements will not result in any unexpected negative impacts;
- Use operational experience and maintenance data to continuously upgrade the program and fine tune it so that optimum results are achieved with minimum expenditure of maintenance resources;
- Compare maintenance experience with each prescribed maintenance performance indicator and use root cause analyses to identify the programmatic reasons for any unsatisfactory findings or trends.

An effectiveness of the root cause analysis program used to support the RCM program will depend upon how well it is able to identify and prevent “maintenance preventable failures”. These are unplanned SSC failures which result from weaknesses in the RCM process.

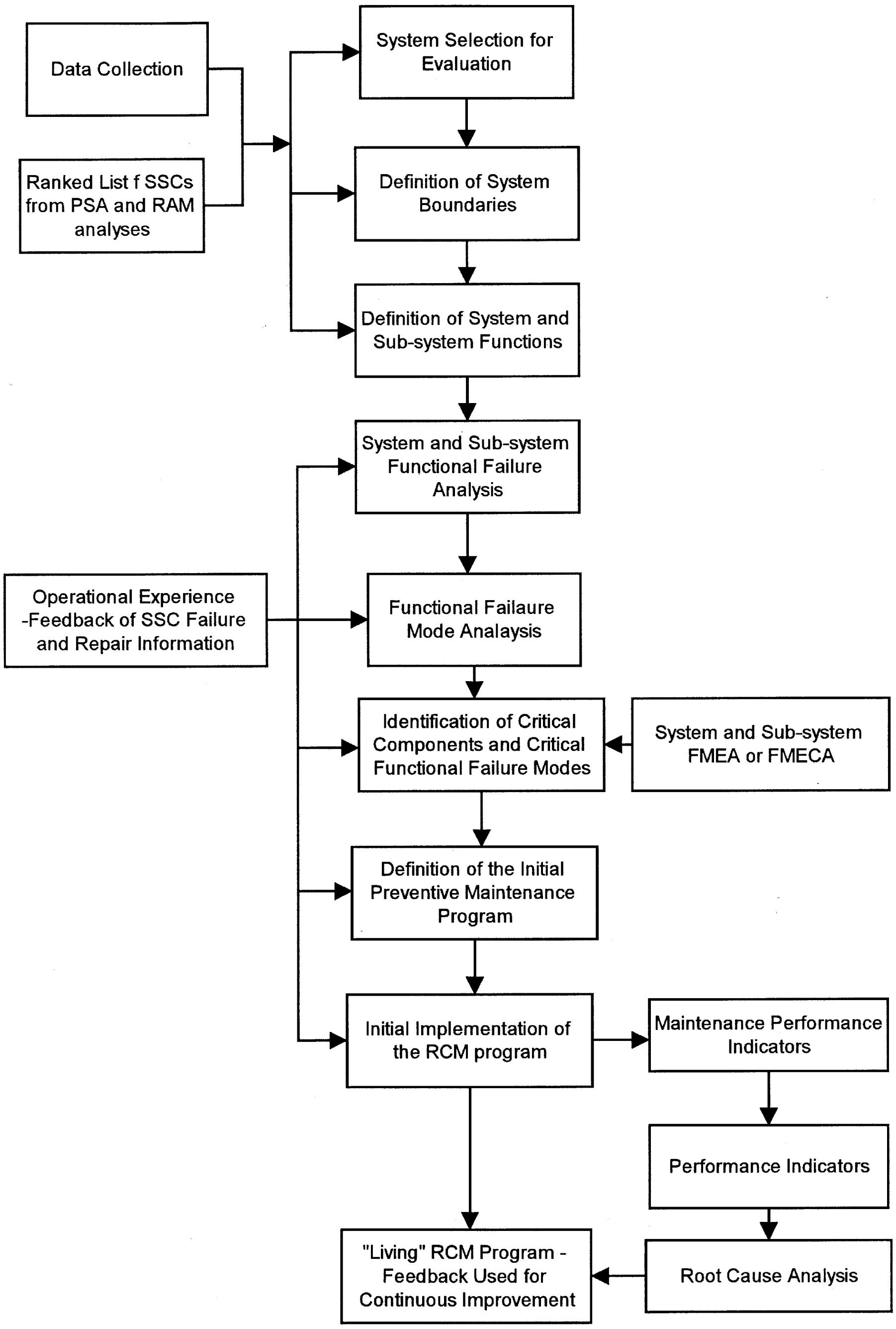

Data Collection
Ranked List f SSCs from PSA and RAM analyses
System Selection for Evaluation
Definition of System Boundaries
Definition of System and Sub-system Functions
System and Sub-system Functional Failure Analysis
Operational Experience -Feedback of SSC Failure and Repair Information
Functional Failaure Mode Analaysis
Identification of Critical Components and Critical Functional Failure Modes
System and Sub-system FMEA or FMECA
Definition of the Initial Preventive Maintenance Program
Initial Implementation of the RCM program
Maintenance Performance Indicators
Performance Indicators
"Living" RCM Program - Feedback Used for Continuous Improvement
Root Cause Analysis

*FIG. 6-3. The RCM process.*

The root cause investigation process supports the RCM program in preventing repetitive failures by looking at very unplanned failure and determining each of the reasons that the RCM program was ineffective.

Some of the possible reasons for the importance of root cause analysis to the continuous improvement of the RCM program include the identification of causes, or reasons that:

- SCC failure mode was not previously identified as dominant or important:
  - ineffective SSC failure analysis (failure mode not recognized or assumed to be unimportant);

  - expected conditions different from those assumed during the SSC failure analysis, i.e. component design, construction, installation or operation not as originally specified so the assumptions made during the SSC failure analysis become invalid (design flaw or loss of design configuration);
- SSC failure mode was identified by the failure analysis, but, the selected preventive maintenance strategies were ineffective;
- Selected preventive maintenance strategies were effective, but, their selected periodicity was inappropriate;
- Selected strategy was appropriate, but, plant staff over-rode, or ignored, the indications and failed to fully implement the selected maintenance strategies for the SSC;
- The selected strategy was fully implemented, but, performed ineffectively, i.e. during performance of the PM task the maintainers initiate an error which negates or reduces the benefits expected from the preventive maintenance activities.

Upon identification of the causes for the experience failure which was “maintenance preventable“, not only will implementation of recommendations for change in management systems and analytical processes result in “continuous improvement“, but, trending the number of failures as a function of time will also provide a high level performance indicator which intimates how well the entire plant maintenance program is performing.

#### *6.3.2.3. Availability (minimum MTTR for unplanned failures)*

In addition to maximizing the reliability of important SSCs, it is also important to examine their associated downtime contributions to determine whether the total out-of-service times were unavoidable or whether they are capable of improvement with better planning, enhanced maintenance processes or improved SSC maintainability.

The investigation into the causes of out-of-service contributions to SSC unavailability provides a new opportunity to use the plant root cause investigation capability. It does so by focusing the investigation on the relationships between institutional and organizational activities and specific maintenance activities and determining exactly what actually happened during the repair process and where delays were initiated or propagated.

When the average SSC down time is within normally accepted levels for a particular maintenance activity, the need for a formal root cause analysis may be lessened and a structured interview or “post mortem“ can be used as a surrogate approach to identify potential process improvements.

If significant delays were experienced during the repair process, i.e. the repair or total down time exceeded normal expectations, a formal root cause investigation should be initiated.

This RCA should use informal or structured interviews and data collection techniques to obtain the needed information from the maintenance team members charged with performance of the work. From this information, the O-RAP maintenance investigator should be able to:

- Identify each discrete functional task, and its individual contribution to time required to complete the overall SSC repair and restoration process;
- Develop a “time line“ which describes each event which took place during the repair and restoration process;

- Identify each critical maintenance event on the maintenance time line, i.e. those events, which had they been prevented or done more effectively, would have significantly reduced the overall down time associated with the failure;
- Identify the management system weaknesses or failures which resulted in the delays which manifested themselves in the form of an increase in the expected down time; and
- Develop and implement recommendations to change the way in which the maintenance management systems, specific and other similar maintenance activities will be performed in the future to prevent the occurrence of similar unwanted repair delays.

### *6.3.2.4. Maintainability*

Component maintainability can be numerically equated to the probability that a failed SSC will be repaired and restored to service within a specified period of time, under a specified set of conditions. Some of the important influences on SSC maintainability are described below, because they must be considered both during the design and operational phases of plant life. SSC down time can be allocated to several discrete steps in the repair process:

- Time needed to isolate, de-energize and drain the system in preparation for the work. The time required will be affected by:
  - round-the-clock availability of operators to isolate and tag-out the SSC,
  - whether predefined isolation and tag-out boundaries exist,
  - whether operators have easy access to drain valves, vent valves and proximity to plant drains to take potentially contaminated fluids.
- Time needed to staging and preparing the work site for SSC disassembly. This time requirement will be affected by:
  - availability of approved procedures and qualified and trained maintenance personnel,
  - availability of spare parts, special tools and/or the need to install scaffolds or rigging,
  - time taken to install temporary shielding the remove interferences.
- Time needed to perform the work:
  - whether the SSC protection system prevents consequential damage,
  - whether poor working environment decreases worker efficiency, i.e. inadequate heat, light, ventilation or excessive requirements for use of personal protective equipment,
  - SSC has inherently low maintainability (complex, hard to disassemble).
- Time needed to restore the SSC at the completion of maintenance:
  - complex or difficult fill, vent and re-energization procedures,
  - complicated post-maintenance tests or inadequate testability.

The interrelationships between each of the important generic contributors to delays in maintenance are shown graphically in Figure 5-9.

#### 6.3.2.4.1. Maintenance planning to minimize SSC unavailability

The degree and effectiveness with which each maintenance activity is pre-planned can have an important impact on the magnitude of the generation losses which occur during every forced, maintenance and planned outage. Since implementation of the most effective management systems and definition of the best possible programmatic approaches are the element of RAP which ensures “continuous improvement“, it is important that these self-same standards are employed to minimize the maintainability contributions to SSC unavailability during every outage.

Since information is key to the successful achievement of the O-RAP objective, once again the foundation for improvement comes from the selection of a “best possible“ approach to maintenance planning, followed by a combination of effective outage monitoring and root cause investigative activities which set the stage for the identification of changes which will assure “continuous improvement“ in maintenance planning.

In the case of maintenance planning, there are two major categories of events for which the “best possible“ approach should be developed:

- Planning for events which provide an unexpected opportunity to perform maintenance and remove required activities from the plant’s living list of maintenance activities which are awaiting a plant shutdown;
- Planning for maintenance, refuelling and modification outages.

The more work that can be done during the former of the first category described above, the smaller the potential work scope and associated outage duration, which can be expected during the second category of event.

6.3.2.4.2. Planning for unplanned outages

Though this may seem to be a contradictory statement, it is intended to imply that there is a need to have a planned outage schedule for needed maintenance activities which either require a plant shutdown, or are preferably performed during shutdown because they carry an attendant risk of initiating a plant upset or failure when performed “on-line“.

One approach which appears to promise an effective return on the resources expended in the planning process can be described as follows:

Step 1: Maintain a “living“, active, list of all pending maintenance, calibration, inspection and testing activities which require a plant shutdown. This list will be derived from a combination of insights and requirements provided by:

- The plant’s preventive and predictive (condition directed) maintenance programs,
- The plant’s in-service inspection and testing programs,
- The plant’s surveillance testing program,
- Regulatory requirements and commitments.

Step 2: Develop and maintain several outage schedules:

- An eight-hour schedule, which focuses on work that can be done by either the operating or maintenance staff within an eight hour period;
- A twenty-four hour schedule, in which the first eight hours are represented by the eight hour schedule;
- A three-day schedule, in which the first twenty four hours are represented by the twenty-four hour schedule.

Step 3: Pre-stage each of the maintenance tasks which are included in the three day schedule:

- Develop the required maintenance packages and assemble all needed procedures and any associated logistical needs (spare parts, special tools) in a controlled holding area which can be readily accessed on demand;
- Confirm that all required tools, calibrated instruments or maintainer certifications are currently available;
- To the extent possible, perform the necessary area radiation surveys and define the requirements for any radiation protection needed to perform the work;
- To the extent possible, prepare any permits which may be needed before the work can be initiated;
- Clearly define the requirements for any needed post-maintenance functional testing and prepare any needed procedures or documentation.

Step 4: Implement the schedules on short notice, whenever there is an unexpected plant trip or shutdown:

- Immediately enter the eight hour schedule;
- The eight-hour schedule should focus on work which can be done by either the operators or maintainers because it is possible that initially there will be a shortage or maintainers on site who are able to perform the work, particularly if the outage occurs outside the normal day-work hours;
- As soon as the plant operators determine that the plant will not restart within eight hours, initiate the twenty-four hour schedule;
- As soon as the plant operators determine that the plant will not restart within twenty four hours, initiate the three-day schedule.

Step 5: Develop a schedule for any additional work that can be done during the outage, should it exceed three days.

Implementation of the planning process described above should ensure that any available plant down time, no matter how short, can be exploited in reducing the amount of maintenance backlog which is awaiting shutdown conditions.

The last remaining task, which is very important, involves a detailed review of the results of the outage, to determine where delays occurred and where improvements could have been effected with prescience.

#### 6.3.2.4.3.. Spare parts management

The plant spare parts program is an essential part of the overall O-RAP because it ensures that there will always be an adequate supply of spare parts on hand when they are needed and that the plant will never experience costly delays in repairs while awaiting spare parts. However, maintaining this inventory can also result in significant additional costs to plant operation if it is not optimized. A general approach towards inventory optimization is provided in the remainder of this section of the O-RAP guide.

An effective spare parts management program has several broad objectives:

- Ensure that the spare parts inventory contains at least one of every part which is likely to be needed to effect repairs to an important SSC whose failure results in an unacceptable impact on plant safety or production;
- Ensure that the "on-hand" complement of spare parts for each important SSC piece part is sufficient to prevent any unacceptable losses in plant or safety system availability which would follow the occurrence of more than one failure during a typical inventory replenishment cycle;
- Maintain the necessary inventory at minimum or optimum cost.

Historically, inventories have contained several different classes of spare parts, each of which tends to have its own individual analytical requirements when decisions are made about whether to stock, and how many:

- Very expensive spare components or large assemblies for important SSCs, e.g. reactor coolant pumps, large motors, large pumps, turbine generator rotors, generator exciters, unit and service transformers, etc.;
- Expensive controlled (safety related) piece parts and complete assemblies for important SSCs, e.g. ECCS pump internals, reactor feed pump internals, valves and operators, instrumentation, control and actuation system components;
- Expensive industrial grade (non-safety related) piece parts and complete assemblies for important SSCs, e.g. condensate and feedwater pumps, valves and controls, breakers, small transformers, non-safety instrumentation, control and actuation system components;
- Smaller generic parts needed to maintain important safety related SSCs, e.g. bolts, fasteners, gaskets, cables, connectors;
- Commercial grade parts needed to repair and refurbish failed SSCs, e.g. bolts, fasteners, gaskets, cables, connectors;
- Safety and non-safety grade consumables, e.g. grease, oil, gasket material, valve packing.

In managing the cost of inventory the first important step must involve the application of a "graded QA" program. Because safety related parts cost up to 300% more than their corresponding commercial grade equivalents and incur significantly higher costs from maintaining their pedigree and environment during storage, it is essential to limit the number of parts classified as "safety grade" to a minimum, i.e. those parts whose reliability is important to the prevention of functional failures in SSCs which the PSA studies show to be important to risk and safety. After the graded QA program has been implemented and the Basic Cost of Individual Spare Parts is held to its optimum level, the next task is to optimize the actual number of spares which are purchased for on-side inventory.

#### 6.3.2.4.4. Spare parts inventory

The spare parts classification scheme described in the previous section above can provide a focusing mechanism which can be used in the management of the overall plant spare parts inventory. This classification process is further described by the following:

– Very expensive spares ($1 million to $30 million)

Decisions to purchase one, or more, of these very expensive parts must be justified on a case-by-case basis using reliability assessments and detailed economic analyses. These analyses generally use the following approach:

- Calculate the expected annual failure frequency for at least one of the installed plant components of the type undergoing analysis, using actuarial information from appropriate industry databases,
  Frequency = failures/year = (1/MTBF) * (hours/a) * (number of like components)
- Determine a realistic best estimate for the expected duration for a full or partial plant outage if the failure were to occur. This will be based on the expected lead time for replacement or, if feasible, the time taken to borrow a component from another generating plant;
- Calculate the expected outage cost from the expected duration and predicted revenue losses;
- Calculate the average annual economic risk, from not having a spare available;
- Calculate the cost of maintaining a spare on-site — typically this represents an annual cost which approximates 25% of the purchased spare part cost.
  Note: this is not the first cost, but the annual carrying cost which is derived from the out-of-pocket expenses of maintaining a storage and inventory management system and the lost opportunity cost of the money used to purchase the spare — first cost is only important if the spare is never used and has a salvage value at the end of plant life.

If the spare is purchased to minimize plant planned outage costs over its lifetime, or has a benefit in reduction of some or all planned outages, in addition to its providing insurance against failure, these benefits must be explicitly addressed in the economic analyses.

The above demonstrates how an analysis can be performed to justify the purchase of a single spare. When should the plant purchase more than one spare?

The decision to purchase more than one spare will be based on information derived from various sources, the two most common of which are:

- The probability of the plant experiencing common cause or two near-simultaneous non-independent failures and the ensuing costs from generation losses:
  - Annual economic risk is calculated from the frequency of (near) simultaneous failures of more than one like component AND the cost of the outage resulting from having insufficient available spares;

  $risk = (#CCF pairs * CCF/a) * ($Loss/Event)
  $loss/Event = MW reduction * Hrs/Lead Time * $ /MW-Hr
- The probability of having a second independent failure during the period that the plant has no on-site spares because it is in the replenishment cycle following the first failure and the ensuing costs from generation losses:
  - Annual economic risk is calculated from frequency per year of one failure AND the probability of a second failure during the replenishment period AND the costs

of the outage which results when no spares are available to mitigate the effects of the second failure;

| | | |
|---|---|---|
| \$risk | = | (#components*1/MTBF*h/a) * (1/MTBF * h/lead time) * (\$loss/Event) |
| \$loss/Event | = | MW reduction * Hrs/Lead Time * \$/MW-Hr |

The present lifetime worth of this risk is equated to the cost of purchase of the second spare and the magnitude of the resultant cost benefit ratio used to justify its purchase. Analyses of this type can be quire expensive and are typically only done for individual, very expensive parts.

– Controlled safety related and industrial grade piece parts and complete assemblies for important SSCs.

These parts are represented by the more common inventories of expensive safety related or utility critical components. A general approach which can be used to determine an appropriate inventory and complement for them is shown in Figures 6-4A and 6-4B. The highlights of this approach are as follows:

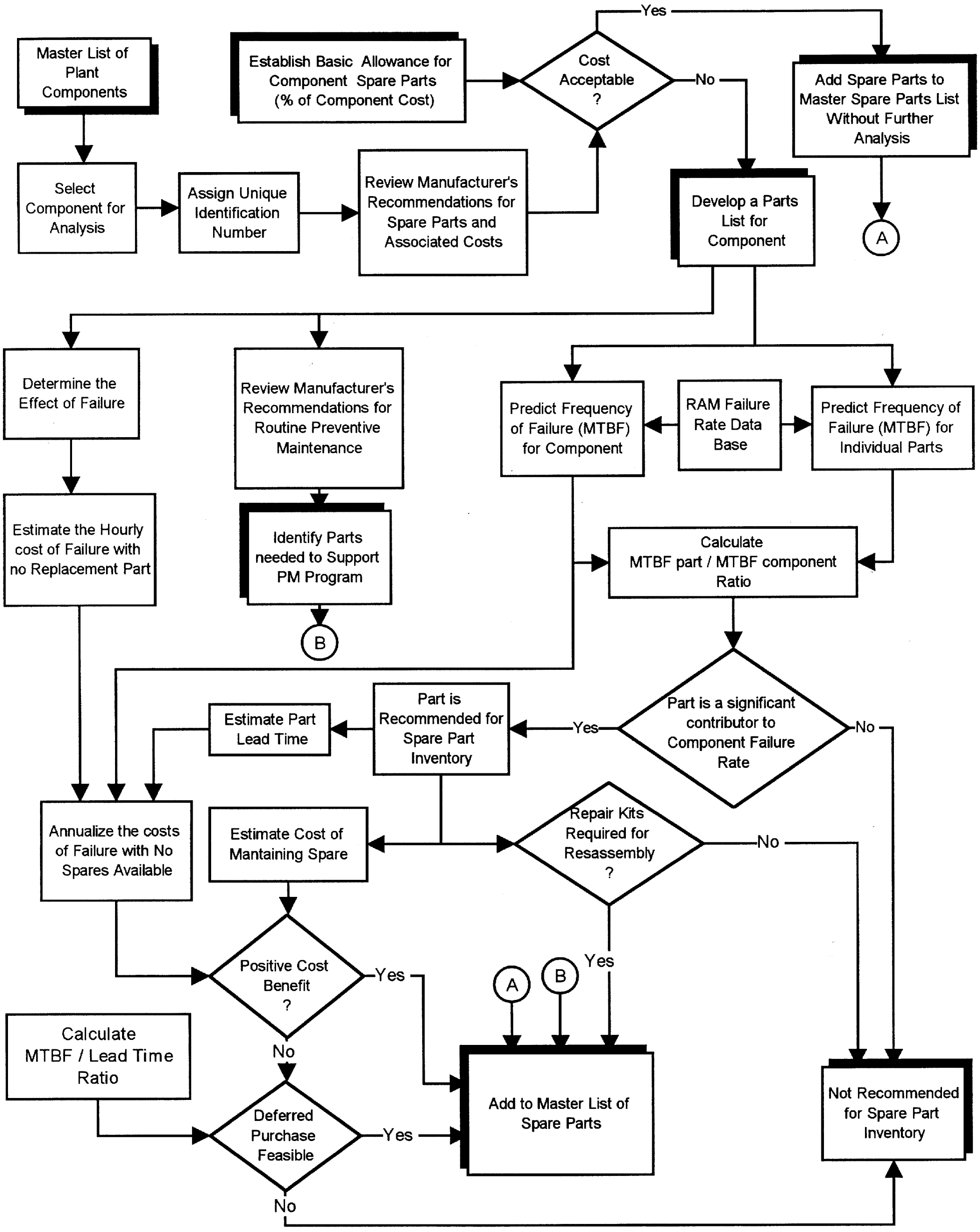

Master List of Plant Components
Establish Basic Allowance for Component Spare Parts (% of Component Cost)
Cost Acceptable ?
Yes
No
Add Spare Parts to Master Spare Parts List Without Further Analysis
Select Component for Analysis
Assign Unique Identification Number
Review Manufacturer's Recommendations for Spare Parts and Associated Costs
Develop a Parts List for Component
A
Determine the Effect of Failure
Review Manufacturer's Recommendations for Routine Preventive Maintenance
Predict Frequency of Failure (MTBF) for Component
RAM Failure Rate Data Base
Predict Frequency of Failure (MTBF) for Individual Parts
Estimate the Hourly cost of Failure with no Replacement Part
Identify Parts needed to Support PM Program
Calculate MTBF part / MTBF component Ratio
B
Estimate Part Lead Time
Part is Recommended for Spare Part Inventory
Yes
Part is a significant contributor to Component Failure Rate
No
Annualize the costs of Failure with No Spares Available
Estimate Cost of Mantaining Spare
Repair Kits Required for Resassembly ?
No
Positive Cost Benefit ?
Yes
A
B
Yes
Calculate MTBF / Lead Time Ratio
No
Add to Master List of Spare Parts
Not Recommended for Spare Part Inventory
Deferred Purchase Feasible
Yes
No

*FIG. 6-4 A. Spare parts optimization process (determination of inventory).*

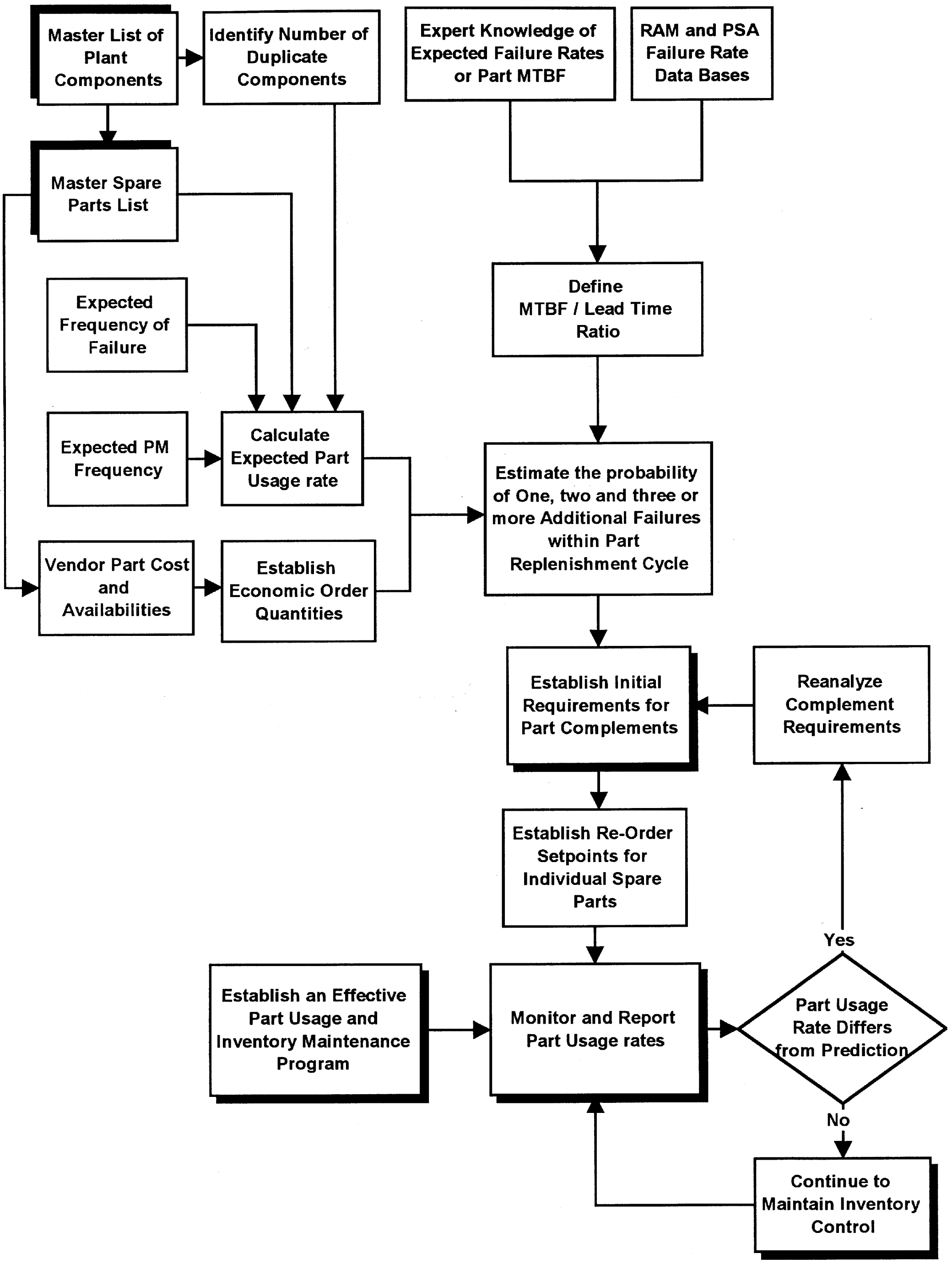

Master List of Plant Components
Identify Number of Duplicate Components
Expert Knowledge of Expected Failure Rates or Part MTBF
RAM and PSA Failure Rate Data Bases
Master Spare Parts List
Expected Frequency of Failure
Define MTBF / Lead Time Ratio
Expected PM Frequency
Calculate Expected Part Usage rate
Estimate the probability of One, two and three or more Additional Failures within Part Replenishment Cycle
Vendor Part Cost and Availabilities
Establish Economic Order Quantities
Establish Initial Requirements for Part Complements
Reanalyze Complement Requirements
Establish Re-Order Setpoints for Individual Spare Parts
Yes
Establish an Effective Part Usage and Inventory Maintenance Program
Monitor and Report Part Usage rates
Part Usage Rate Differs from Prediction
No
Continue to Maintain Inventory Control

*FIG. 6-4 B. Spare parts optimization (determination of complement).*

**Initial screening on the basis of cost**. Because it is both expensive and time consuming to perform a detailed spare parts analysis, it is desirable to devise an initial assessment technique which allows an automatic pass through of the vendors recommended spare parts list on the basis of cost, i.e.

- If the recommended spare parts for a particular component cost less than some percentage (10%) of the component cost, accept the recommendations "as is",
- If the cost of the recommended spares exceeds the limit, but, the overage is dominated by one or two single parts, it may be possible to analyse the need for these few expensive spares and then accept the remainder "as is".

**For the remainder of the spares review process**, the following tasks are required to define spare parts inventory and complement.

- Determine inventory, i.e. which parts will be stocked:
  - Develop a parts list, if not already provided in detail by the vendor as part of the bill of materials or other procurement documents;
  - Use the plant RAM and PSA databases and the projected equipment operating profile to predict the annual frequency for component failure and the relative importance of individual failure modes;
  - Equate the actuarially derived failure modes to the piece parts associated with their failure and repair, and estimate the ratio between the component MTBF and the MTBF from these individual piece parts;
  - Identify those parts which are important because they dominate the unreliability of the component and recommend that they be considered for addition to inventory;
  - Determine the scope of additional parts, not involved in the failure, but required in the reassembly process and add them to the master spare parts list;
  - Determine the likely extent of consequential damage which could be expected to accompany the occurrence of the more probable failure modes and confirm that the spare parts list has sufficient scope to achieve an effective repair.

    Note: The issue of severe consequential damage is often accommodated by maintaining complete spare sub-assemblies on site, in addition to individual piece parts. The economic evaluation process used to prioritize and justify spare assemblies will parallel that used to justify the inclusion of all other parts in the inventory.
  - Calculate the average annual expected economic risks which result if the spare part under analysis is unavailable at the time of SSC failure, using:
    - the expected frequency of part/component failure,
    - the hourly costs which are incurred while the part remains in the failed state,
    - the minimum expected duration of the event calculated from the minimum reliable replenishment interval, i.e. the minimum amount of time which should provide a high level of assurance that a replacement part can be obtained from the vendor, other power plants or any other identifiable source.
  - Calculate the annual average costs of maintaining the spare in inventory.

    Note: this will not be the first cost but will reflect:
    - time value of money (lost opportunity cost) for the budget expended on purchase of the spare,
    - cost of maintaining the inventory — storage facilities, labour, heat, cooling, etc.
    - any effects (positive or negative) on the overall economic costs which result from the influence of local taxation practices and depreciation of assets.
  - Compare the average annual risks of not having a spare with the costs of maintaining it in inventory to guide the decision to purchase, or not to purchase.

The process described above appears to be time consuming and cumbersome and likely to add significantly to the burden of stocking a new inventory. In reality, a large number of analyses will be repetitive and individual assessment can exploit information which is of a similar nature, calculated for other parts. It must be remembered that the calculations are to guide the selection of parts for inventory, and accuracy is not always important, providing any approximations are adequately conservative.

**Deferred purchase**

It is possible that the costs of maintaining a part in inventory are high, the benefits from having the part are marginal, and there is a great deal of confidence that its purchase can be delayed, i.e. if failure occurs, the commonly encountered failure modes indicate that it is very unlikely that it will be needed for several years. In this case, it may be possible to defer purchase for some period of time. The evaluation can proceed on two bases:

- Initial screening on the basis of MTBF/Lead time ratio. If the part has a very long MTBF and a short lead time, deferred purchase may be possible on the basis that part failure is highly unlikely, when it occurs it may be detectable before SSC functional failure, and the part can be obtained quickly;
- Detailed economic evaluation using time dependent (non constant) failure rates.

6.3.2.4.5. Spare part complement

Following a determination that a particular part should be carried in inventory, the next question to be answered is one how many parts the inventory should contain. Part complement is determined from its expected usage rate and the economic risk associated with allowing a depleted inventory to occur during the part replenishment cycle which would otherwise follow the removal of parts from stock. factors which influence usage rate and complement include:

- part failure rate and usage rate per component,
- number of similar components.

This provides the annual usage rate. However, to control handling charges and to exploit the substantial discounts offered by some vendors for multiple purchases, many smaller parts have “economic ordering quantities”. Both of these factors are considered during the determination of complement in which the analyst calculates the probability of incurring additional failures during the re-order and inventory replenishment cycle.

After the initial assessment of inventory, the plant must carefully monitor trends in part usage rate and optimize the inventory. There are several commercially available software programs to assist the plant in achieving this optimization process for on-hand spare parts complements.

An alternative formulation of the spare part complement determination is proposed below. In this approach, the benefit from selecting each component spare is calculated from the change in component mean down time (MDT) which is directly attributable to its being available when needed. As defined earlier, the MDT represents the total time required to restore a failed component to operability. This MDT has two components:

- The time needed to remove and replace the component spare, and,
- The expected delay which would follow while obtaining a replacement, if it were not available at the time it is needed.

The probability that a spare is not available when needed will be a function of the number normally held in inventory (complement), the number of like components and their reliability (part usage rates) and the time taken to restock parts after they have been removed from inventory (replenishment cycle).

When the RAM analysis has shown a component to be a candidate for inclusion in the spare part inventory because it has a high importance measure, the benefit from maintaining spares can be calculated by varying the associated mean down time and measuring its effect on the plant equivalent forced outage rate (EFOR). When the replacement power costs exceed the costs of maintaining the part in stock, it should be included in the inventory. When the part usage rate is calculated from the number of similar components and their failure rates and compared to the length of the part replacement cycle, it is possible to calculate the probability that a needed part will not be available.

This information can be used to modify the unavailabilities for the affected components in the RAM model and a series of sensitivity studies performed to determine the optimum sparing level, i.e. the minimum number of parts stored on-side which provides adequate assurance that a critical component will not be unavailable for lack of a needed spare part. There are a number of commercially available computer based programs which help the decision maker perform these needed calculation.

### 6.3.3. Reliability/availability/maintainability improvement (RAMI)

The primary objectives for the RAMI plant will generally include the following:

- Identify systems, structures and components (SSCs) which are potentially significant contributors to generation losses or important to risk and identify those whose potential for improvement, i.e. increased reliability, availability or maintainability, may warrant the expenditure of betterment funds;
- Identify all important trends in plant and SSC performance and identify areas of possible improvement;
- Consistently identify the causes of individual performance problems and define effective remedial measures which remove, or prevent their re-occurrence;
- Consistently predict the worth of proposed improvements to guide the justification and prioritization process for plant modifications and changes, and optimize expenditures to provide the greatest benefit within the shortest periods of time;
- Provide an overall framework for maintaining a well documented and risk optimized plant configuration which prevents the inadvertent violation of any of the prescribed deterministic or probabilistic criteria or commitments which are part of the plant design basis.

The RAMI program consists of a set of management systems and processes which provide the individual “success paths” needed to achieve the above objectives. The output from this program will be a “living” improvement plant which consists of prioritized and justified current and proposed corrective actions designed to achieve an optimal level of plant reliability, availability and maintainability. The program will periodically provide an integrated documented summary of all aspects of plant performance to guide the overall plant management process.

#### *6.3.3.1. “Living” rank-ordered list of SSCs for safety and economy*

The basis list of rank-ordered SSCs will be derived from the results of the RAM and PSA analyses performed for the final reference plant design. The ordering process will exploit the individual characteristics of each of the commonly encountered importance measures and will be used to guide the performance driven enhancement program. The initial ordering process, however, is founded on the “expected” contributions to unavailability and unreliability. After the plat goes into operation and the subsystems mature, it is important that the list is re-ordered to reflect actual plant operating characteristics. This will be achieved from periodic updates of the RAM and PSA models to reflect any hardware or system changes and the actual contributions which individual SSC failure rates and restoration times make to SSC failure rates.

The primary tool used to update the “expected” to “actual” plant SSC failure rates and restoration times will be a formally implemented procedure which exploits all of the information gained about plant failures. The updating process should be “Bayesian” in nature, although merely using statistical pooling and establishing new failure distributions with their attendant dispersion parameters may be insufficient because of changes to the sample population. This population may changes as the plant matures, because:

- When influences on SSC performance from plant management systems are recognized, changes will be made to correct and enhance them wherever necessary. The effects from this database attribute will be manifest as a continuous trend in reduced SSC unavailability and unreliability;
- When design flaws are recognized and the service factors for individual SSCs are changed by modification, individual failure modes may be eliminated from practical concern. Contributions from these failures must be screened from the database if its statistical analysis is to be used as a predictor of future SSC performance;
- SSCs are generally replaced with “like kind” components, although during the life of the equipment the manufacturer may introduce new materials, new manufacturing techniques, new control and protective schemes or modified designs which actually enhance the SSCs ability to withstand the effects of individual failure mechanisms;
- SSC failure rates are not necessarily constant. The composite functional failure rate for an SSC represents the aggregate rate for a set of individual failure mode specific rates, each of which is affected differently by fault finding and fault correcting test and maintenance activities. This carries the implication for potential long term increases in failure rates which may, or may not, be reset to “as new” or “as was” at various times in plant life.

The implication from the above is that though “Bayesian” updating process may reflect the best method for achieving real time predictors of future performance for individual SSCs, the distributions should be manually changed whenever there is evidence for a change in the characteristics of the population from which the statistics are drawn, i.e. there is a caveat, implicit to the database updating process, that knowledge about improvements should be incorporated into the update at the time they are recognized, and not deferred until much later when their effects become manifest by the observed failure and repair data for individual SSCs.

The database should be updated on a periodic basis (e.g. once per year).

#### *6.3.3.2. PSA and RAM model updating*

As the plant matures and changes in hardware and management systems and processes are implemented to reduce the effects of important failure modes, mechanism and repair processes, the PSA and RAM models must be changed to reflect them, if they are to remain useful as a predictor of future safety and economy. This means that there must be a formal process imposed to ensure that all changes to the plant are periodically incorporated. This can generally be done in one of two ways:

- Making the RAM and PSA maintenance teams part of the modification decision-making process, i.e. ensure that they make a formal assessment of the expected benefit for each proposed modification and become part of the implementation organization. At least, to the extent that they are notified at the completion of each change so that the PSA and RAM models can be updated on a continuous basis to keep them current with actual plant configuration;
- Review each engineering package which was approved for implementation during the annual refuelling and maintenance outage and make all of the necessary changes to the RAM and PSA models which reflect these changes.

In each case, the work required to maintain the PSA and RAM models may appear burdensome, but, after the first two or three operating cycles, very few modifications can be expected to have a major impact on the RAM and PSA models. Generally, unless a modification involves changes in dependency, redundancy, diversity or success criteria the PSA model will change very little over time. The primary changes to the PSA and RAM analyses will involve the quantification database, which should also be updated on a periodic basis, e.g. once per year.

The RAM and PSA models should be requantified and re-solved with this enhanced database to provide an updated list of rank-ordered SSCs which can be used to better prioritize the expenditure of resources earmarked for improvement programs during the coming year.

This same quantification and associate PSA results can also be used to provide time dependent plots of the probabilistic performance criteria and provide an additional set of high level plant performance indicators.

### 6.3.4. Ageing management of ALWRs

#### *6.3.4.1. Introduction to the effects of nuclear plant ageing*

In the current application of PSA, the failure rate data used in the quantification process is generally assumed to be time independent. There is evidence, however, to show that as plant components age they will experience a gradual acceleration in failure rate which, if unchecked could result in significantly higher levels of plant risk. Because periodic equipment overhauls generally reset the "ageing" clock for important SSC failure modes, scheduling these overhauls can have an important impact on risk. To determine the best strategy for managing ageing induced changes in risk, it is necessary to both understand how ageing affects the reliability of individual components, and how the effects of this information can be transformed into risk-related information by the plant PSA.

There are two characteristic ways in which the effects of ageing influence the failure probabilities of both active and passive components:

- As an increase in the failure rates for active and passive component piece parts which are initiated by "wear-out".

Any increase in the failure rate of an individual component piece part can only result from either an increase in the effective magnitude of the loads imposed upon it, or a decrease in its ability to withstand those loads, i.e. a decrease in its strength.

Some of those more common manifestations of "wear-out" which lead to chronic increases in material stress or decreases in material strength are listed below:

- Erosion (thinning), compression or distortion of load bearing members which results in increased static and dynamic material stresses with normally applied loads;
- Material erosion, compression or distortion which results in changed clearances between moving surfaces;
- Degradation in material properties (e.g. thermal and radiation, embrittlement, strain hardening or fatigue) which cause reductions in strength or increases in the probability of stress induced brittle failures;
- Reduction in integrity (e.g. cracking, pitting), often caused by the effects from corrosion or erosion/corrosion. These mechanisms result in a reduction in the effective load bearing capability of a load bearing member.

- As an increase in the unavailability of active components caused by an increase in the number or severity of non-functional failures which require remedial attention and removal from service.

Failure rates for passive components and passive piece parts of active components generally increase as they age, however, evidence of the incipient degradation processes often remain undetected and uncorrected during normal operation, because they affect the structural capability of the component rather than its functionality. This means that normal in-service testing programs may provide poor age induced fault detection capabilities and reliance must be placed on the periodic examinations provided by an in-service inspection program. The following are additional examples of faults which are important to component reliability, but, whose degradation provides little or no effect on their functionality prior to failure:

- Embrittlement and cracking of electrical cables which affect their mechanical characteristics and their ability to maintain their integrity and functionality during seismic, fire and flooding events. Their normal electrical capabilities may remain unaffected by the ageing processes;
- Erosion and corrosion of piping systems;
- Radiation embrittlement and cracking of primary system pressure boundaries;
- Fatigue failures of structural components initiated by cyclical mechanical and/or thermal loading.

The importance of increases in passive component failure rates appear to depend on the extent to which structural loading during an accident is different from the loading seen during surveillance testing. When the conditions imposed on the component are the same during both normal operation, testing and accident conditions, the conditional failure probability following an initiating event should be no higher than that seen during testing This means that if failure is imminent, it should be detected during routing testing, particularly if there is any forewarning, e.g. leak before break.

The conditions under which passive failures have potential risk importance include:

- A failure which becomes an initiating event, e.g. a pressure boundary failure which affects the reliability of fluid inventories and in turn results in the loss of one or more success paths maintaining normal plant critical functions;
- When the structural loading of the passive component is significantly greater during accidents than during normal operational activities, and undetected degradation results in an important increase in its conditional failure probability. This implies that passive components exhibit their greatest conditional age related weaknesses during response to plant transients which are initiated by external events which impose acute structural stresses on the component, or where an off-normal condition results in an energy release which in turn introduced loads which can result in catastrophic failure.

  These weaknesses are seldom evidence by degraded function during normal operation, thus will usually remain detectable only through ISI activities. Indeed this observation is consistent with experience, because if accident conditions are more severe than those seen during normal operation or test, the component's failure modes are undetectable by test (test is inefficient) and the period over which ageing induced effects can accumulate can be very large, as can its conditional failure probability.

Examples of passive failures which may have important conditional failure probabilities include:

- Containment, where undetected degradation of the concrete or steel could result in premature failure when challenged by the internal pressure loading expected during a severe accident;
- Electrical cables, where degradation of mechanical properties (embrittlement or loss of flexibility) could result in electrical failure when the cable is exposed to dynamic loads associated with a seismic event;
- Electrical cables, whose loss of mechanical integrity (insulation cracking) could result in electrical failure when they are exposed to water incursion during a flooding event.

When a passive component is exposed to similar conditions during both normal and off normal conditions, its conditional failure probability can reasonably be expected to be so much lower that the conditional failure probabilities for active components in the same success path. This allows the assumption to be made that its contribution to system or success path failure probability is relatively insignificant. The only time that the validity of this statement may be challenged would come when the passive system failure initiates simultaneous failures of multiple, otherwise independent success paths.

Active components were originally thought to be of lesser concern to ageing studies because whenever a critical component experiences a major failure or exhibits unacceptable increases sin failure rate it is repaired or refurbished and returned to relatively “as new” condition. However, studies indicate that the selection of overhaul and inspection intervals and schedules can have a large impact on the importance of age-induced effects on active component reliability and plant risk.

- Active component failure probabilities undergo a cyclical change in reliability which are a function of normal operation (number of starts and operating hours), any age-induced acceleration in failure rates and periodic repair, refurbishment or replacement activities which negate, completely or in part, the effects of ageing;

- Because the time dependent change in failure rates for active components can be several orders of magnitude larger than those seen in passive components, the cyclical variations reliability can be important and can have an important effect on system reliabilities if subsystem, train and system inspections and overhauls are not coordinated to provide the minimum effective age for the system.

**Failure detection and intervention**

Both active and passive components can provide forewarning of failure:

- Active components often show degraded capability, excess heat, or vibration prior to their failure, which can be identified during surveillance testing programs;
- Passive components often show leakage before they fail catastrophically;
- Electrical insulation may show detectable changes in leakage current, resistance or reactance when degradation occurs;
- Piping may experience "leak before break" or exhibit levels of thinning and cracking which are detectable with an ISI program.

This implies that component failure probabilities can have both time dependent and time independent components. Failure rates for active and passive components may increase with time, however the probability of failure to detect degradation prior to complete failure may be constant.

Where the second term becomes important, it must be considered in the calculation.

### *6.3.4.2. Ageing management in ALWRs*

In managing the life-cycle risk for an ALWR, the first step becomes one of defining the rank-ordered list of SSCs which are important to plant risk so that it can be used to focus available resources on performing the activities needed to manage the ageing process for important SSCs.

This of itself can be difficult for the following reasons:

- The failure rates for individual SSCs may be a function of their effective age, i.e. the time since its last test or inspection which indicated it was in "as new" condition,
- The failure rates may be uncertain or unknown,
- The plant overhaul and inspection schedule, which determines the effective age for each SSC may be unknown,
- The process used to incorporate the age-dependent information into the PSA to provide a set of quantitative and qualitative results for each year of plant life can be complex and time consuming.

However, individual SSC ageing rates derived from published results from USNRC's NPAR program and their incorporation into a level 1 PSA for an older PWR indicate that the potential for risk increase is quite significant and preventive measures should be incorporated into the operational RAP.

6.3.4.2.1. Objectives for ageing risk assessment

An ageing risk assessment project could be expected to have several specific objectives:

- Predict variations in lifetime plant core damage frequencies, attributable to specific effects which originate with equipment ageing rates and plant maintenance policies and to assess the importance of ageing mechanisms to O-RAP;
- Identify and rank, in order of their importance to risk, SSCs and associated maintenance policies which are important to the management of age dependent risk;
- Formulate basic strategic which are useful in managing the age dependent reliability and availability of individual components which have an important influence on core damage frequency.

**Selection of the methodology**

Currently, two fundamental approaches can be used to identify nuclear plant age dependent risk, measured in terms of core damage frequency, and rank the individual SSCs which have the greatest influence over this surrogate measure of risk. These two approaches are briefly described as follows:

- Explicitly model component replacement schedules and time dependent effects on component unreliability and unavailability in the level 1 database and simulate the effects, year by year, by completely, or partially resolving the PSA models;
- Manipulate the results (cutsets) from the level 1 reliability assessment within an external ageing assessment risk program. The basis for the statistical methods which can be used with this second approach and methodology is taken from NUREG-1362 and NUREG/CR-5510.

  This latter report document similar work performed for the USNRC by Dr. Bill Vesely, hence the name "Vesely approach" which will be used to characterize the methodology throughout the remainder of this discussion on ageing risk.

**PSA structure**

To fully evaluate the effects of ageing, the influences from the very real effects described above must be incorporated into the estimation of time dependent or asymptotic failure probabilities for each plant component or component piece part which plays an important role in preventing core damage. Since either the models or the results of the level 1 PSA were used as the initiating point for this ageing study, the components which have an important influence on age-induced risk must be included in the PSA models and contained within the resultant cutsets.

All active components which exhibit time dependent failure rates must be included in the ageing study input models or cutsets, particularly if they have unusually long periods of time between overhauls or complete inspections which return them to an "as known" or "as new" condition. To ensure that this is true with the Vesely approach where the level 1 cutsets serve as an important analytical input, the baseline PSA must be reanalysed with a lower truncation value to increase the total number of cutsets and minimize the inadvertent exclusion of components which are only potentially important after the effects of ageing have been included.

The simulation approach requires no special consideration for potential omission of important active components since their age dependent probabilities and frequencies are used in the requantification of the baseline models, hence, inadvertent omission of important active components is not possible.

6.3.4.2.2. Simulating the effects of ageing with the level 1 PSA models

In concept, the simulation approach is the more straightforward of the methods currently available to perform ageing risk assessments. In the simulation process, plant surveillance and overhaul intervals are combined with component-specific failure, repair and ageing rates to calculate the failure probability or failure frequency for each event which is included in the PSA. This activity results in a unique basic event data (BED) base for each year of plant life.

These BED files are used in the requantification of the level 1 models to provide:

- Core damage frequency predictions for each remaining year of expected plant life,
- Sequence importance and contributions to total core damage frequency (TCDF) for each remaining year of plant life,
- Failure event (component and initiating) importance as a function of plant age.

From the results of these calculations it is possible to infer which components are important in controlling age-dependent risk, which components should be the subject of further scrutiny in a series of sensitivity analyses or more detailed future assessments and whether the importance of individual accident sequences or the plant risk profile changes as the plant ages. Plant specific overhaul and test intervals must be used whenever possible because it is the “phase” relationships between overhaul intervals determines the average effective age of each success path and the resultant effects on reliability.

The opportunity to use an actual plant schedule may not be possible early in life so a best estimate ISI and overhaul schedule must be developed and later used to help define the actual plant overhaul schedule. Figure 6-5 shows a flow chart for the “ageing simulation approach with a level 1 PSA”.

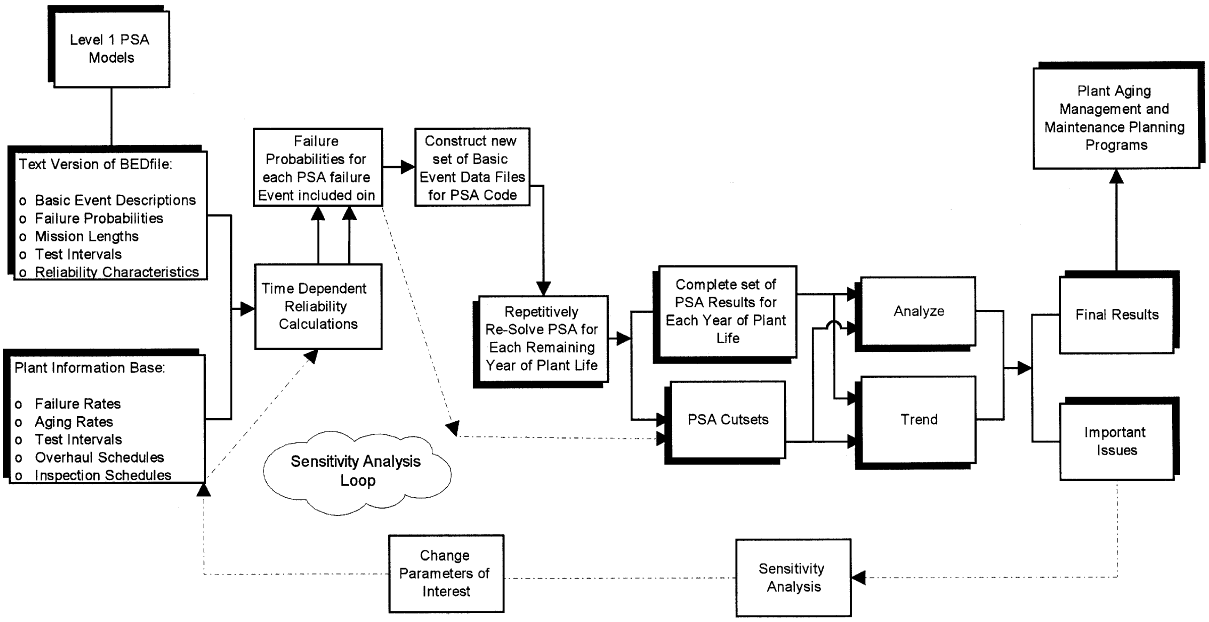

Level 1 PSA Models
Text Version of BEDfile:
o Basic Event Descriptions
o Failure Probabilities
o Mission Lengths
o Test Intervals
o Reliability Characteristics
Plant Information Base:
o Failure Rates
o Aging Rates
o Test Intervals
o Overhaul Schedules
o Inspection Schedules
Failure Probabilities for each PSA failure Event included oin
Time Dependent Reliability Calculations
Construct new set of Basic Event Data Files for PSA Code
Repetitively Re-Solve PSA for Each Remaining Year of Plant Life
Complete set of PSA Results for Each Year of Plant Life
PSA Cutsets
Analyze
Trend
Final Results
Important Issues
Plant Aging Management and Maintenance Planning Programs
Sensitivity Analysis Loop
Change Parameters of Interest
Sensitivity Analysis

*FIG. 6-5. Aging simulation with a plant PSA.*

#### 6.3.4.2.3. Ageing assessment using a statistical approach

The set of accident scenarios, described in terms of their contributing cutsets are the primary inputs required for this method of ageing risk assessment. Calculation of the sensitivity of core damage frequency to each cutset element, both singly and in combination with each other, allows calculation of the change in core damage frequency which could be expected to result from any postulated changes in failure probability for individual failure events. This means that if the time/age dependency for each of the individual factors which influence failure event probabilities or frequencies could be defined, the age dependent effects on component failure probability and, hence, the age dependent character of total core damage frequency could be defined.

The set of reliability parameters for each failure event which is contained within the input database used to calculate age-dependent failure probabilities includes:

- Reliability as a function of time,
- Unavailability as a function of time,
- Surveillance testing, in-service inspection (ISI) and in-service testing (IST) activities,
- Replacement and refurbishment intervals and specific schedules for individually important components.

Because the ageing process potentially affects all components simultaneously, the analysis is structured to look at both individual and combined ageing effects as indicators of relative importance and for overall ship in core damage frequency (CDF). The approach proposed by Vesely is legitimized by its use of a standard Taylor expansion of the core damage equation in which a change in dependent variable can be expressed as a function of the changes in the independent variables. In this case, changes in core damage frequency are expressed as a function of changes in the age related effects on the reliability and availability of each active and passive hardware component whose failure influences the likelihood of core damage.

Delta CDF = Sum (contributions from all individual ageing effects)
(due to ageing) + Sum (contributions from interactions of two ageing effects)
+ Sum (contributions from interactions of three ageing effects)
+ (…. n ageing effects)

Because this expression can be expressed in terms of component specific sensitivity coefficients and ageing induced changes in the unavailability of these components, it is possible to separate the level 1 reliability calculations from the ageing calculations. The sensitivity coefficients for each component or combinations of components can be determined from the level 1 PSA results and the ageing contribution to unavailability from the modified/updated TIRGALEX database (NUREG/CR-5510). A flow chart showing the general process followed during performance of an ageing assessment with the Vesely approach is shown in Figure 6-6.

### *6.3.4.3. Ageing rate database*

#### 6.3.4.3.1. Ageing database development

The starting point and default for an ALWR project database will likely be TIRGALEX, an ageing rate database published in the USNRC's NUREG/CR-5510. Because this database was developed largely from expert opinion at a time when there was little quantitative information available about age induced effects on hardware unreliability, the data can be augmented with information from component specific NPAR studies. Information from NPAR can be used either to confirm that the extant ageing rates in TIRGALEX are appropriate, or to define new values which can substitute for TIRGALEX estimates.

#### 6.3.4.3.2. General applicability of the TIRGALEX database

Because the source data for TIRGALEX is derived from US sources, there may be some concern for its applicability to other non-US nuclear plant databases. However, consideration of the mechanisms and conditions which produce ageing effects make it appear plausible that the time dependent rate of change in failure rates seen for US nuclear plant components can be equally effective in predicting the rate of change of failure rates for non-US plants, provided this acceleration in failure rate is superimposed on baseline database which is plant specific.

#### 6.3.4.3.3. Ageing issues and the applicability of ageing data

Whether ageing rates derived for similar plant components which have different maintenance programs and philosophies can be used with confidence, will depend upon there being a clear distinction between contributions to component failure frequency or probability from ageing, those which are purely the results of "service", and those which are the result of the effectiveness of plant maintenance, test and inspection programs.

Three basis processes which must be understood before the effects of component ageing can be converted into time dependent failure probabilities or frequencies for use in the PSA:

- How age induced change in component failure rates are used to calculate time dependent failure probabilities,
- How the effects of ageing are manifest, so that maintenance dependent contributions can be separated from contributions which result from "service",
- How to determine the applicability of generic ageing rates to plant specific analyses.

## 6.4. ANALYTICAL TOOLS FOR O-RAP

Throughout the O-RA process there is a continuous need to employ investigative processes which identify the critical conditions needed to maintain "continuous improvement" i.e. where problems or losses are occurring, the causes for the losses, and the reasons for their occurrence. The analytical tools needed to support O-RAP and provide insight into the areas where vulnerabilities in design or operational features are similar to those used in D-RAP.

The basic analytical tool chest can be expected to include:

- A baseline level 2 or level 3 PSA which includes:
  - Multiple power states (full power, low power, hot and cold shutdown and mid-loop operation),
  - Internal and external initiating events,
  - Uses a current plant specific database.

- A baseline plant level RAM model which supports quantification of the plant load duration curve and prediction of SCRAM frequency and uses a current plant specific database;
- A "fast-solver" level 1/2 PSA for full power and shutdown operating states and internal initiators to be used as an "engineering tool". Ideally, this PSA will:
  - Be an integrated single model (rather than multiple event and fault trees which must be merged and reduced to provide estimates of core damage frequency),
  - Have all local faults modularized (constructed to locate all local faults in independent sub-trees),
  - Reflect the true plant dependency network,
  - Have a user interface designed for engineering applications,
  - Use a current plant specific database.

  Because this fast-solver PSA will also be used to establish the relative and absolute importance for failure events which occur during plant operation, a graphical user interface should be provided to minimize the changes or error and mis-applications by non-PSA specialists.

  Note: A fast solver PSA which includes external initiating events may also be necessary if they dominate the risk profile for the ALWR.

- A (near) real time level 1/2 PSA (full power and shutdown) which can be used to provide risk based information to the plant operating staff and guide the management of operating plant configuration:
  - Integrated single model,
  - Local faults modularized,
  - True dependency network,
  - Probabilistic contributions from test and maintenance removed,
  - User interface designed for operators and outage managers,
  - Capable of calculating time dependent instantaneous risk from a plant outage schedule (on-line and shutdown maintenance),
  - Use a current plant specific database.

- Individual system reliability and availability models which can be used to perform detailed engineering analyses which support the optimization of test and maintenance and justify and prioritize detailed system improvements;

- Individual SSC failure models which were developed during D_RAP and in the application of RCM and maintained current to assist in the identification of important failure modes and to support the root cause investigation process.

In addition to the plant level models, there will also be a collection of "ad hoc" models which have been developed or derived from one of the above and specifically tailored to meet a very specific application.

## 6.5. O-RAP PLANT INFORMATION AND DATABASE

Because the information collected to characterize plant state and current performance provides inputs to virtually all of the O-RAP management processes, its quality, applicability and timeliness will have an important impact on the degree to which the O-RAP is successful in meeting each of its defined objectives. Some of the more important aspects and attributes of this plant-wide data collection system are provided in this section of the guide.

### 6.5.1. Plant operating and maintenance information system

When establishing a performance monitoring system several broad steps should be taken to assure its effectiveness in meeting each of the possible user needs. Important amongst these steps are:

- Uniquely, and formally, identifying each plant SSC and its associated functional and non-functional failure modes so that all potential users of information relating to the SSC have a common, and unambiguous basis for communication;
- Defining each potential root source of SSC performance information, i.e. the sources of raw data from which all other need information will be inferred or derived;
- Cataloguing the information needs for each user department, commonly performed in the form of a user matrix;
- Defining the individual information processing methods, techniques and tools which convert the raw data into a form needed by a specific user;
- Developing an implementation plan which assures the most cost effective translation of raw information into the minimum set of informational elements needed by the user organizations to meet their individual plant decision making and reporting requirements.

When this information collection and analysis system is implemented it should assure that:

- All users have access to consistently identified and recorded sources for all levels of plant performance data (plant, system, sub-system, component and piece part);
- All redundant data collection systems are eliminated and that additional requirements for periodically imposed special “ad hoc” data collection programs are minimized;
- Manual efforts required to assembly information for specific reports to outside agencies and internal management organizations are minimized;
- The timeliness of internal and external reporting is improved.

Figure 6-7 was developed to demonstrate how few sources of raw data there really are from which to infer plant performance. This figure shows the general sources of data which originate from on-line SSC failures and how this information can be processed with actuarial, statistical and probabilistic analytical techniques, methods and models to provide a wide range of decision making and performance monitoring support.

A similar information collection and analysis process can be derived for shutdown plant conditions and for planned outages.

### 6.5.2. Unique identification numbering system

It is essential that the plant must have an effective and comprehensive unique identification numbering system if all performance related information is to be unambiguously attributed to each SSC in an accurate and consistent manner and all users of the information are able to assure its pedigree. This system can be arbitrary, i.e. developed for plant specific applications, although modern-day data reporting programs tend to require specific formats. Unfortunately, since each external reporting system has specific objectives its requirements may not be broad enough, nor detailed enough, to meet all plant specific needs. This implies that the unique ID systems have the following general characteristics:

- Broad enough in scope to include all plant SSCs and even their associate piece parts;
- "User friendly" so that the identifier carries as much intelligent information as possible, i.e. results in an identifier which may have up to twenty characters, yet can be readily understood "at a glance" by all potential users;
- Contains enough information to satisfy all potential users, i.e. if vendor and failure mode specific databases are needed by individual users, the identifier contains the requisite identifiers for sorting purposes;
- Be suitable to also provide the basis identification numbering system for the spare parts program and to store and retrieve information in the equipment history record system.

One system which is used in the United States which meets many of the requirements identified above, is the energy industry identification system (EIIS), defined by IEEE Standard 803, although any comparable standard issued by an individual Member State will likely suffice. The selection process for any standardized approach will probably be dominated by the ease with which its format can be adapted to satisfy the requirements of formal reporting processes imposed by outside agencies.

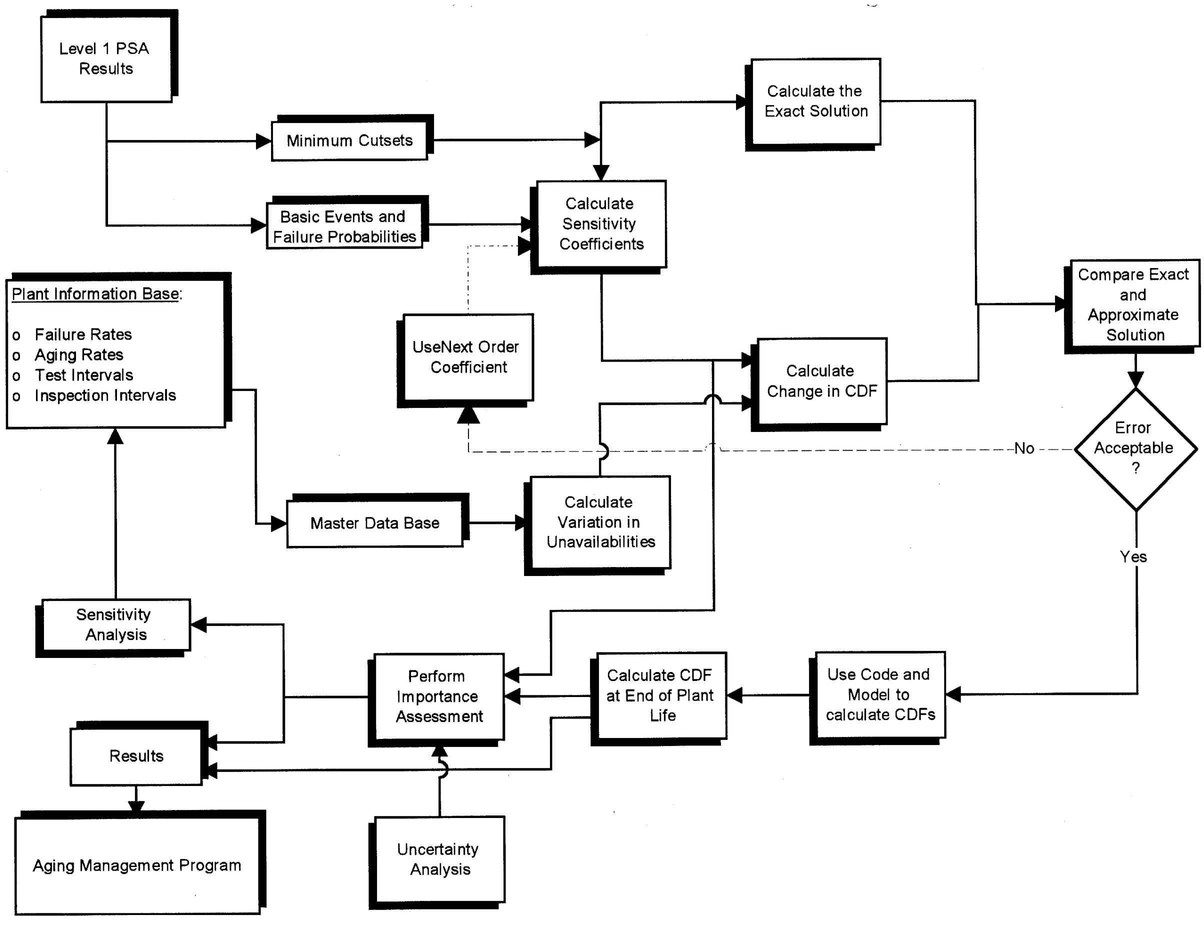

Level 1 PSA Results
Minimum Cutsets
Calculate the Exact Solution
Basic Events and Failure Probabilities
Calculate Sensitivity Coefficients
Plant Information Base:
o Failure Rates
o Aging Rates
o Test Intervals
o Inspection Intervals
UseNext Order Coefficient
Compare Exact and Approximate Solution
Calculate Change in CDF
Error Acceptable ?
No
Yes
Master Data Base
Calculate Variation in Unavailabilities
Sensitivity Analysis
Perform Importance Assessment
Calculate CDF at End of Plant Life
Use Code and Model to calculate CDFs
Results
Aging Management Program
Uncertainty Analysis

*FIG. 6-6. Agling assessment using the Vesely approach.*

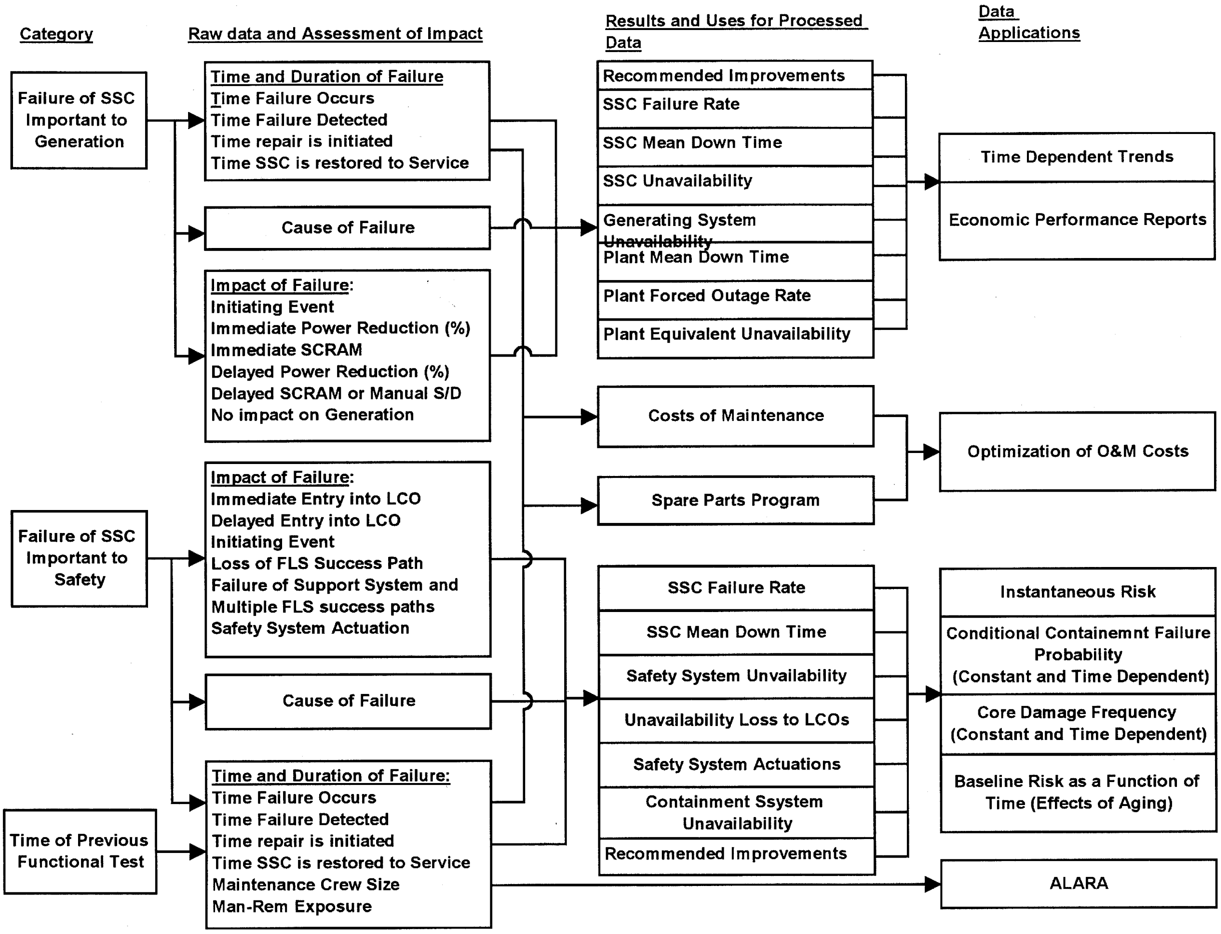

Category
Raw data and Assessment of Impact
Results and Uses for Processed Data
Data Applications
Failure of SSC Important to Generation
Time and Duration of Failure
Time Failure Occurs
Time Failure Detected
Time repair is initiated
Time SSC is restored to Service
Cause of Failure
Impact of Failure:
Initiating Event
Immediate Power Reduction (%)
Immediate SCRAM
Delayed Power Reduction (%)
Delayed SCRAM or Manual S/D
No impact on Generation
Recommended Improvements
SSC Failure Rate
SSC Mean Down Time
SSC Unavailability
Generating System Unavailability
Plant Mean Down Time
Plant Forced Outage Rate
Plant Equivalent Unavailability
Time Dependent Trends
Economic Performance Reports
Costs of Maintenance
Spare Parts Program
Optimization of O&M Costs
Failure of SSC Important to Safety
Impact of Failure:
Immediate Entry into LCO
Delayed Entry into LCO
Initiating Event
Loss of FLS Success Path
Failure of Support System and Multiple FLS success paths
Safety System Actuation
Cause of Failure
Time of Previous Functional Test
Time and Duration of Failure:
Time Failure Occurs
Time Failure Detected
Time repair is initiated
Time SSC is restored to Service
Maintenance Crew Size
Man-Rem Exposure
SSC Failure Rate
SSC Mean Down Time
Safety System Unvailability
Unavailability Loss to LCOs
Safety System Actuations
Containment Ssystem Unavailability
Recommended Improvements
Instantaneous Risk
Conditional Containemnt Failure Probability (Constant and Time Dependent)
Core Damage Frequency (Constant and Time Dependent)
Baseline Risk as a Function of Time (Effects of Aging)
ALARA

*FIG. 6-7. Operational data collection (at-power).*

An **example** of a typical **unique identification numbering system** is provided below:

**Unit/system/component/part/generic description/manufacturer/train**

**XX – XXX – XXX – XXX-XXX XXX XXXX XXXXX – XX – XX**

The generic description can provide a precise functional description of the component using a predefined set of identifiers which, for a pump (based on NPRDS), may include:

| | | | | | | |
|---|---|---|---|---|---|---|
| Pump type - | (a) | - | Axial | (e) | - | Reciprocating |
| | (b) | - | Centrifugal | (f) | - | Radial |
| | (c ) | - | Diaphragm | (g) | - | Rotary |
| | (d) | - | Gear | (h) | - | Vane Type |
| Inlet size - | (a) | - | Under 2” | (d) | - | 12” – 17.99” |
| | (b) | - | 2” – 5.99” | (e) | - | 18” – 28” |
| | (c ) | - | 6” – 11.99” | (f) | - | Over 28” |

Materials (body) – predefined list

| | | | | | | |
|---|---|---|---|---|---|---|
| Type of shaft seal: | (a) | - | Packing gland | (d) | - | Canned (no seal) |
| | (b) | - | Mechanical | (x) | - | other |
| | (c ) | - | HP fluid injection | | | |
| Specific speed: | (a) | - | under 4000 | | | |
| | (b) | - | 4000 – 7000 | | | |
| | (c ) | - | Over 7500 | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Flow capacity: | (a) | - | under 500 gpm | (d) | - | 10,000 – 50,000 gpm |
| | (b) | - | 500 – 2499 gpm | (e) | - | over 50,000 gpm |
| | (c ) | - | 2500 – 9999 gpm | | | |

| | |
|---|---|
| Total developed head | Actual head in feet |
| Flow rating | GPM |
| Speed at rated capacity | RPM |

### 6.5.3. Equipment history and reporting

The accurate and timely reporting of data is critical to the long term success of O-RAP. One important source is the equipment history card, which provides a concise description of the "cradle to the grave" experiences associated with each individual component. Though originally, actual cards were generally developed for each piece of equipment, presumably, this same information would now be recorded directly into, or drawn from, a computerized database. The information which should be recorded and associated with each piece of equipment should generally include the following, although some of the inputs, e.g. reliability data, could be derived from other operational inputs by the computer.

- **Engineering data**
  - Component and part identification shown in "exploded view",
  - Description of equipment, its operation and design capabilities,
  - Maintenance specific information, i.e. procedures which govern all preventive and corrective maintenance activities, including lubrication schedule and approved lubricants,
  - Specific parameters needed to maintain the equipment in "operable" condition, such as required clearances, hot and cold alignment data and protective system set points.

- **Reliability data**
  - Recent failures and their failure modes, their root causes and past maintenance actions,
  - Service since last failure (operating hours, starts, tests and operational demands),
  - Initiators of common cause failures and confirmation that they are/are not functional failures.

- **Repair data**
  - Free field, or pre-formatted menu, description of work completed,
  - Identification of parts which were replaced, repaired or adjusted,
  - Failure cause (by code or description),
  - Time of failure detection and time restored to operability,

  - Type of failure- functional, incipient,
  - Time and man-hours expended by maintenance.

- **Consequence data**
  - Decrease in plant output, SCRAM or manual shutdown and MW-Hr loss,
  - Safety system unavailability (train/system/function) or accident sequence initiating event (precursor).

As an adjunct to this computerized equipment history "cards", the database can also be used to initiate any required documentation for withdrawal of spare parts from inventory, and to reproduce any needed procedures on demand. This latter use of the database is particularly valuable because it provides a means for procedural configuration management, whereby only the master procedure in the database need be maintained. The entire system can be established on a Local Area Network, within which the equipment related information is identified and accessed through a "home page".

### 6.5.4. Risk-based performance indicators

One of the prime goals in an effective risk-based management program is to provide the facility manager or oversight organization with a tool that can be used routinely to provide insights into the current facility risk profile, and to identify any trends which are likely to be indicators of degraded "safety" or increased risk.

Ideally a "living" facility risk assessment will provide guidance on how to estimate or monitor the trend in facility risk. The question which follows, is one of how this can best be achieved.

There exists a limited set of functional variables which relates operational parameters and the importance of operational events to the risk which the facility presents to its workers, the general public and the surrounding environment. If each of these parameters and their relationships to risk and routine plant state information can be predicted, then the resulting insights can provide the basis for a comprehensive risk-based performance indicator program.

In the assessment of facility risk, there are several discrete functional contributors which play a role:

- Frequency of events which initiate accident sequences,
- Reliability of barriers which are used in the confinement/containment of the radiological hazard (fuel clad, RCS, containment),
- Expected consequences from a failure to confine the radiological hazard (fission products),

  This latter contribution is a function of:
  - The damage state for the facility following a barrier failure which may affect,
    - The magnitude or concentration of the released hazard,
    - The duration of the hazard release,
  - The likelihood that potential targets (public, staff or environment) can be protected following a failure to confine or contain the hazard.

The goal for a risk based performance indicator program is to identify the set of available operating facility information provides inferences of undesirable trends in each of the above functional areas, and utilize the existing risk assessment to either:

- Determine, "a priori" the points where action must be taken to correct undesirable trends, or,
- Estimate the significance of identified trends to determine the need for remedial actions.

The potential information which can be used in each area will be described, and from that an attempt will be made to identify specific “performance indicators“.

### 6.5.5. Initiating event frequency

Accident initiating events have a single common characteristic that may represent a de facto definition, namely, that the event leads to a loss of one or more functions which must be maintained to keep the facility in its normal operating mode or state.

The loss of a normal function results from one or both of the following:

- Loss of capability of a success path which is maintaining the required function, resulting in a transition to a new facility operating state. Such a loss normally results from a functional failure of one or more of the process functional elements.
- Loss of integrity of the process system boundaries, which leads either to a loss of success path function or to an immediate loss of confinement of the process hazard.

Any facility event or changing condition which affects the frequency of occurrence for either of the above must become an immediate candidate for surveillance as a risk-based performance indicator (RBPI).

Before this information can be used in an RBPI program, relevant and appropriate plant informational parameters must be identified. The following preliminary list is an attempt to provide this identification for each class of initiating events.

- Process transients
  - In-process transients, or upset conditions which result from the loss of functional capability of a process element and necessitate a change in the facility operating state. These are typified by step changes in process throughput, including plant shutdown, which are required to mitigate the effects of functional failure of the normal process.
    In the ALWR, these conditions are represented by SCRAMs or immediate reductions in power, which follow the failure of some part of the normal heat generation or heat rejection hardware.
    Note: The cause is not important, and can result from hardware or human induced failures.
  - Events which are external to the process, but which lead to an in-process transient condition, typified by loss of a vital support system, such as a failure to supply external power, cooling or process feedstock,
  - Failures which lead to loss of available support systems which increase the probability of occurrence of either 1 or 2, above,
  - Component functional failure resulting from the inadvertent or improper actuation of protective equipment (individual hardware protective trips).

  The performance measure which is appropriate for each of the above can be represented by the reliability of each of the required normal operating functional elements.

  The **indicator** for the reliability is the **number of failures** which are experienced **per unit time** for all normally operating process systems which cause or threaten a loss of a critical process function, i.e. those parts of the system, which if they fail, cause failure of the process. Failure represents the point at which functional capability is reduced to the point that the process fails, and is not necessarily “totally“ failed.

- System or process integrity.
  Boundary components (pipes, ducts, conveyors, conductors) are required to be functional because they provide the transport function within the process. These components are typically “passive“ in nature and failure usually results from a loss of integrity.

Any information which indicates a reduction in the reliability of the components is a candidate for an RBPI.

In summary, potential RBPI’s for initiating events are:

- Reliability data (number of failures per period, or time between failures) for critical operating components or process elements (a human performing operations within the normal process may become a functional element),
  - failure history from maintenance records,
  - reports of human failures (errors).
- Evidence for the functional capability of critical operational elements,
  - surveillance test data,
  - operational parameter trending.
- Data providing the rate of occurrence for failures which result in spurious actuation of protective systems,
- Reliability data for passive components (e.g. number of failures of the process boundary), or the collection of data from which a prediction in failure probability can be made.

In each of the cases above, SCRAM (reactor trip) or process shutdown data may provide most of the needs, although the goal is to be able to infer the rate of occurrence for initiators. Many events which only increase the potential for a process failure may have an effect on the future likelihood of process failures, and as a result, information on failures which threaten process failure should be collected.

## 6.6. SELF-EVALUATION AND ITS ROLE IN O-RAP

An important source of feedback about the effectiveness of the plant management systems which are part of RAP can be obtained from periodically performed self-evaluations or self-assessments. The organizational units performing these self-evaluations compare their actual performance with the expectations prescribed by either individual industry or plant initiatives and implement change wherever needed to raise below normal performance to required levels.

*Self evaluations*

It is very important that formally established criteria are used to guide the self-evaluation process, if it is to provide a steady source of reliable information for improving the effectiveness of each management system which is important in meeting the O-RAP objectives. These criteria fall into four areas, the first involves identification of areas in which there are program weaknesses, the second involves the identification of the causes for those weaknesses and the development of remedial actions which will result in a broad improvement, the third involves the pro-active use of operational experience to help in the identification and resolution of potentially important issues, and finally to benchmark overall plant performance with other organizations to find and emulate “best practices“. Some of the more important criteria in the first category, identification of program weaknesses, include:

- Communicating to all plant staff, an expectation that the self-evaluation program will result in “continuous improvement“ and that self-evaluations will be used by individuals at all levels in the plant organization;
- Self-evaluations are to be treated as an integral part of every daily activity and should be used to examine work processes and work activities to identify improvement actions wherever possible;
- In particular, managers should frequently monitor and influence personnel performance by direct observation of work activities and training, identify adverse cultural symptoms, such as complacency;
- Self-assessment reports must be clear, concise, share relevant information on strengths and areas for improvement and use performance indicators as a basis for identifying areas where improvements are needed.

In the second category, important criteria to be used in guiding the identification of causes and corrective actions for weaknesses uncovered by self-assessments will include:

- Investigation of the causes for important or repetitive problems or adverse trends in performance of non-consequential events which may have plant-wide implications;
- Initiating investigations promptly to exploit the availability of information and evidence, using personnel who have appropriate knowledge and skills;
- Using formal root cause analysis techniques to identify the causes, not symptoms, of the identified problem and initiation of a formal tracking process which will assure the implementation of recommended changes and the sharing of lessons learned with the remainder of the nuclear industry;
- Performance measures and performance evaluations are used to periodically assess the effectiveness of the corrective actions which result from root cause investigations.

In the third category, criteria for using operational experience will include:

- Making sure that operating experience is available to all station personnel;
- Implementing requirements for all levels of the organizatiuon to use industry and plant level operating experience to resolve current problems, anticipate potential problems, and capitalize on information gained from lessons learned;
- Periodically assessing the effectiveness with which plant staff are using operational experience to anticipate and resolve problems.

In the fourth category, in which the program is benchmarked against others, the criteria for self-evaluation will include:

- Communicating the expectation that staff will compare their own performance with that of other organizations to identify, exploit and emulate industry “best practices“;
- The use of performance measures to monitor progress towards achieving desired improvements.

# 7. RELIABILITY ASSURANCE PROGRAMME ORGANIZATION

## 7.1. INTRODUCTION

It is appropriate to consider how the RA programme might be staffed and how the organization directly involved in the implementation of the RA program might interact with each other plant organizational entity whose activities influence plant reliability, safety or risk.

A suggested organization would be one in which a multidisciplinary and technically expert RAP team, which has no direct line responsibilities, exists as a stand-alone organization which can provide reliability and availability engineering services and other forms of technical support to each plant organization which falls under the RAP umbrella. Overall RA program implementation could be achieved under the direction of a high level RAP committee which represents each line and support organization whose responsibility falls within the purview of RAP.

The ultimate success of the RA programme will hinge upon the ability of each participant in the oversight process to communicate freely and to make decisions, i.e. be willing to identify and air problems openly and have sufficient authority to make decisions in behalf of their organization to commit any resources that are needed.

## 7.2. DEFINING THE D-RAP ORGANIZATION

Selection of the RAP organization hinted to above, and further described by the following, is founded upon the following observations.

- All members of the project design engineering team must be fully aware of the overall objectives for the RA program, how each element of the D-RAP integrates with their own activities, and how the tasks which are a normal part of their scope of supply are changed when they come within the D-RAP;
- The development and application of PSA should be the responsibility of the safety and licensing department since it forms an integral part of the combined deterministic and probabilistic safety case. The D-RAP organization has the responsibility for ensuring that the PSA activities are integrated into the overall RA programme and that they are effectively used in the optimization of the plant;
- Though each design team may not have a RAM or PSA specialist, it is important that the department have its own internal group which can focus on how to structure itself to meet its obligations towards improved plant reliability and availability and how to conduct its own internal affairs and expend its own resources in a way which fully embrace each of the precepts of a plant-wide comprehensive RA programme;
- Past experience gained during the implementation of plant-wide Availability improvement, risk based management and reliability centered maintenance programmes has shown that the critical need for expert technical support is best be served when it is provided by a dedicated group of RAM, PSA and data analysts. These specialists are able to use past experience and specific expertise to develop and use the necessary analytical tools, document each analysis so that it is reviewable and reproducible, and presentation all RAM and PSA results and insights in a form which can be used directly by the design or plant operational teams.

A plant level D-RAP organization with three distinct participatory levels appears capable of best addressing each of these issues.

### 7.2.1. D-RAP organization — the D-RAP technical group

The RAP technical group provides the technical underpinnings to the D-RAP and consists of a team of RAM, PSA, economic appraisal and other analytical specialists who act as an expert group or subject matter experts who can be assigned responsibility for the development and application of reliability or risk based analyses and provide particular expertise in RAM and economic assessment to the project design team. This team of specialists will have experience in performing each of the analytical tasks which are an integral part of each of the five basic RA program Elements. The following are typical of the **breadth** and **depth** of the **capabilities** which are often needed within the RAP technical group. Some of these capabilities are required on a day-to-day basis, other more specialized capabilities will be needed by the group on an occasional basis, often needed to assist in resolution of important questions raised during a root cause analysis or by specific reliability enhancement issues.

- Data collection, database development and analysis to support RAM and PSA activities,
- Development and application of baseline and "fast solver" RAM and level 1, 2 and 3 PSAs, for both internal and external initiating events and all applicable reactor power states,
- Deterministic analysis to understand system transient behavior, system success criteria and severe accident phenomena,
- Reliability and maintainability Engineering assessment to provide predictions of hardware reliability, maintainability and availability and to develop appropriate design goals for important SSCs,
- Fracture mechanics and failure analysis to confirm proper material selection in the hardware specification and procurement process,
- Information and human factors review to confirm that the man-machine interface is optimal for human actions which are important to plant safety and economy,
- Economic evaluations to establish the "worth" of changes which affect plant safety and productivity (generation).

A range of expertise could be brought into this group to serve in either an advisory role or to augment staff during periods of peak man-power loading. Within this organizational construct, the RAP technical group will:

- Develop and provide a set of implementing D-RAP procedures to augment the procedures and practices normally used by the design team,
- Serve as an internal consultant where in-depth expertise is required for RAM and PSA technology,
- Develop RAM models which parallel the plant design provide qualitative and quantitative information to the design team,
- Review design decisions to confirm that the inclusion of RAM and PSA information in the design decision making process was appropriate, within the correct context and adequately documented so that the plant reliability and risk basis is well established,
- Coordinate and document all RAM, risk and reliability studies undertaken to resolve unique plant issues,
- Maintain and periodically or continuously update all plant RAM models to ensure that they always reflect current plant design and operational basis.

### 7.2.2. Implementation of D-RAP

Implementation of the overall D-RAP will involve a wide participation by members of the project design team, over and above that represented by the group of dedicated technical specialists described above. Each organization which has a vested interest in achieving the plant reliability, availability and safety goals must be involved in each aspect of the design decision making process and have the opportunity to both represent their own specific interests and to accept responsibility for incorporating RAP precepts within each of their own individual programs and activities.

It can be expected that individual departments will interact directly with the RAP technical group, which in turn will work with them in applying existing RAM and PSA tools to meet their specific needs and applications. The specialist and line organizations will develop the protocols, procedures and general practices which are used to guide the actions of its members in applying RAP in each of their activities.

### 7.2.3. D-RAP committee

There is also a need for a high level interdepartmental, interdisciplinary committee to provide overall guidance, direction and organizational coordination for all plant wide RAP activities. This committee would meet periodically to:

- Review and approve proposals to modify system, sub-system or component reliability and availability goals;
- Compare the allocated plant, system and component level goals with the performance predicted by the design;
- Review the results of all major RAM or PSA studies and confirm their applicability to the plant decision-making process;
- Establish and review policies which guide the development of individual department level RAP activities, review the RAP implementation procedures for each department to assure consistency in approach and objectives;
- Review RAP activities performed within individual departments or organizational units;
- Identify programmatic weaknesses and successes in D-RAP;
- Facilitate integrated interdepartmental responses to specific reliability, availability or risk issues;
- Review all proposals to resolve reliability and availability issues which have an impact on safety or economy;
- Review the D-RAP managers report describing the status, progress problems and successes with RAP.

Figure 7-1 describes how this committee might interact with other organizations and provide the leadership and direction needed to implement a full scale D-RAP. Figure 7-1 provides an overview of potential interactions between the department level organizations, each individual D-RAP element and the skills and capabilities which the RAP technical group needs to provide.

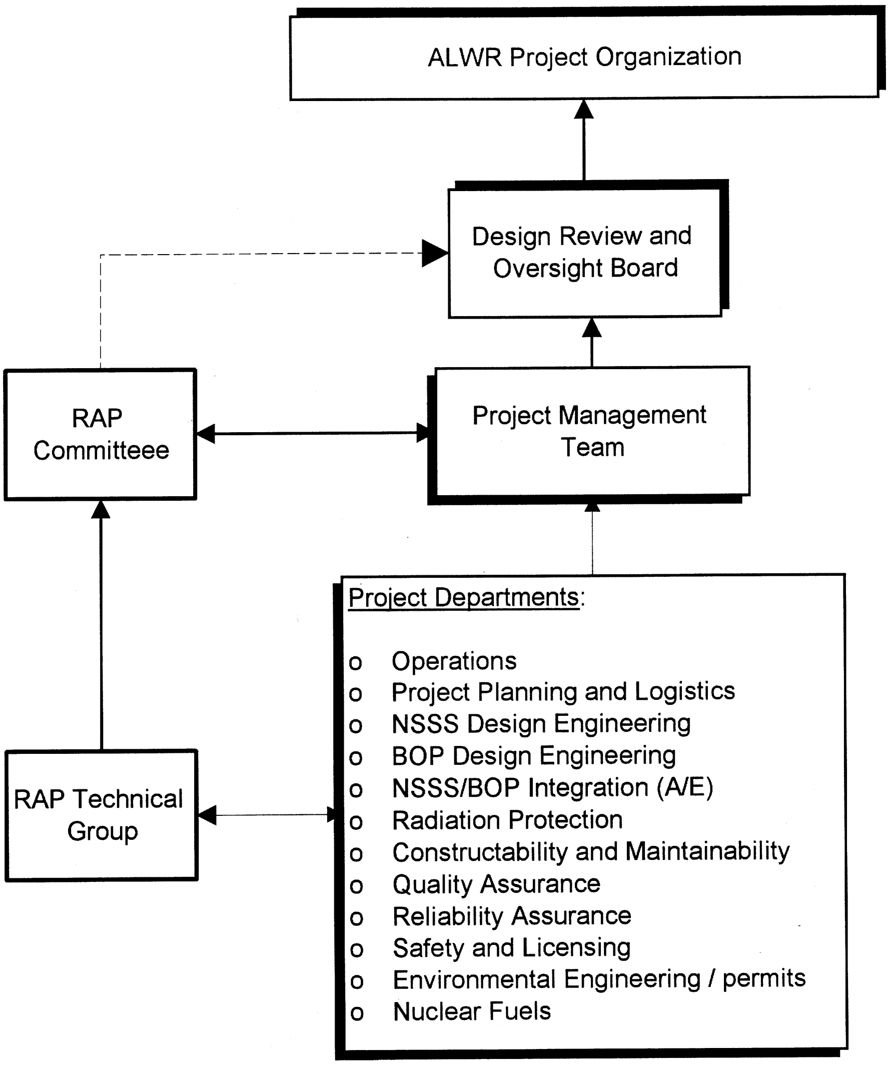

ALWR Project Organization
Design Review and Oversight Board
RAP Committeee
Project Management Team
Project Departments:
o Operations
o Project Planning and Logistics
o NSSS Design Engineering
o BOP Design Engineering
o NSSS/BOP Integration (A/E)
o Radiation Protection
o Constructability and Maintainability
o Quality Assurance
o Reliability Assurance
o Safety and Licensing
o Environmental Engineering / permits
o Nuclear Fuels
RAP Technical Group

*FIG. 7-1. D-RAP organizational structure.*

## 7.3. THE O-RAP ORGANIZATION

During the operational phase, the recommended RAP organization will generally mirror the structure suggested for the design phase, i.e. a strong technically expert group which will develop and quantify the models used to predict the worth of changes to the plant, lead the development and implementation of methods and techniques needed to support each aspect of the O-RAP and to transfer the necessary technology to individual plant staff members who will incorporate them into their own activities. In many cases, this technology transfer may be training, presentation of analytical findings or in the form of expertly derived check-lists and procedures which can be followed by non-specialist staff members.

Overall programme integration and direction would come from the O-RAP committee, except that the nature of the activities performed by this group would shift towards the timely resolution of all reliability and availability issues which impact plant operation, either by affecting risk or capacity factor or by threatening the plant's ability to meet safety and productivity goals.

The primary difference between the O-RAP and D-RAP organizations lies more within the details than within the structure. The types of expertise needed to analyze plant events and improve operating plant procedures and practices will differ from those needed during the design process. The emphasis on being able to fix specific hardware problems will increase and move from a predictive mode to a retrospective viewpoint, i.e. less focus on why something may fail, but, a less abstract assessment of why it actually failed.

### 7.3.1. The O-RAP technical group

The RAP technical group would continue to perform the same kinds of activities initiated by D-RAP, except that in addition, the team will use all sources of plant information to identify sources of lost generation and their causes and coordinate their activities with individual plant line organizations to identify changes which will prevent their re-occurrence. This will require the development of effective root cause analysis techniques and methods and the training of the cognizant plant staff members in their use and the development of ways to quickly and effectively assess the significance of operating events so that resources applied in their resolution are commensurate with their importance.

The RAP technical group will have responsibility for ensuring that the analytical models, methods, techniques and tools used by the production team to provide timely results which have adequate fidelity and accuracy to be used in each desired application. The tools used in the O-RAP will differ from those used in the D-RAP because the conditions surrounding their use will change.

The need to use PSA in routine day-to-day activities means that not only must it solve in a timely manner, but also, when it is used to manage plant configuration it must be modified to exclude probabilistic estimates of unavailability contributed by to test and maintenance activities and expanded to include, implicitly or explicitly, each and every component which may be subject to maintenance. In addition, these tools must either be updated continuously, or on a periodic basis, to reflect the actual “as built” and “as operated” plant condition and configuration, i.e. they must be updated to reflect all modifications, changes to plant procedures and actual plant-specific human and hardware performance.

The individual activities which the O-RAP technical group can be expected to perform, will include:

– Develop and provide a set of implementing O-RAP procedures to augment the procedures and practices normally used by each organization which performs activities which influence the reliability, availability or maintainability of SSCs. Affected departments or organizations are typically represented by the following:
  (i) Results engineering, i.e. compilation and reporting of statistics detailing each aspect of plant performance,
  (ii) Maintenance, i.e. diagnostics, preventive, corrective and planning, equipment history,
  (iii) Operations, i.e. event significance, risk based operational management,
  (iv) Root cause analysis, failure diagnostics, surveillance test and inspections,
  (v) Design engineering, i.e. modifications,
  (vi) Training, i.e. simulation of accident sequences and emphasis on RAM for SSCs,
  (vii) Technical support and emergency planning, i.e. planning for important accident, sequences and the use of PSA for Severe Accident management,
  (viii) Radiation safety, i.e. impact of worker protection on maintainability.

- Serve as an internal RAM, RAP or PSA consultant whenever in-depth expertise is required,
- Ensure that the validity, fidelity and accuracy of the PSA and RAM models is maintained by updating them whenever the plant changes to provide all the necessary qualitative and quantitative information for the design team. The responsibility for maintaining and updating the "living" PSA should be retained by the safety and licensing group,
- Review all design decisions to confirm that the inclusion of all RAM and PSA information in the design decision making process was appropriate, within the correct context and adequately documented so that the plant reliability and risk basis is well established,
- Perform and document all RAM, risk and reliability studies undertaken to resolve unique plant issues.

### 7.3.2. Implementation of O-RAP

The implementation process for O-RAP will evolve from the process initially established during D-RAP, and will change only to the extent needed for O-RAP to meet the new requirements and challenges which appear as the plant makes its transition from design to operation. These changes will be quite extensive in the operational and maintenance departments. In addition to performing their routine tasks, O-RAP organizations will collect information which provides feedback on how well they are achieving their RAP goals by providing the means to quantify individually organization-specific performance indicators and correct all identified programmatic weaknesses which the performance indicator trends identify.

### 7.3.3. The O-RAP organization

O- RAP will be directed by a committee which is made up from representatives of line organization which has an influence on, or responsibility for, plant reliability and safety, in a way which is similar to that used in D-RAP. The members of the O-RAP committee will change as the plant moves into its operational phase, although the functional objectives for the committee will be similar.

Figure 7-2 provides an overview of potential interactions between department level organizations, each individual D-RAP element and the skills and capabilities which the RAP technical group, the technical specialists, need to provide. This is intended to hint at the scope and breadth of the analytical skills which may be needed to provide the requisite technical support to a comprehensive O-RAP.

## 7.4. CONCLUSION

Insights provided by the above discussion of the plant hierarchy from plant objectives to plant organizations leads to a proposition that any organization wishing to implement a formal reliability assurance programme will require a fully capable support group which is able to transfer the needed technical skills to existing line organizations, define the processes needed to assure the implementation of the basic tenets of RAP, provide procedural and technical guidance where needed, and develop and apply the tools, techniques and methods which are an integral part of the quantitative decision making processes which makes RAP so different from many other plant programmes.

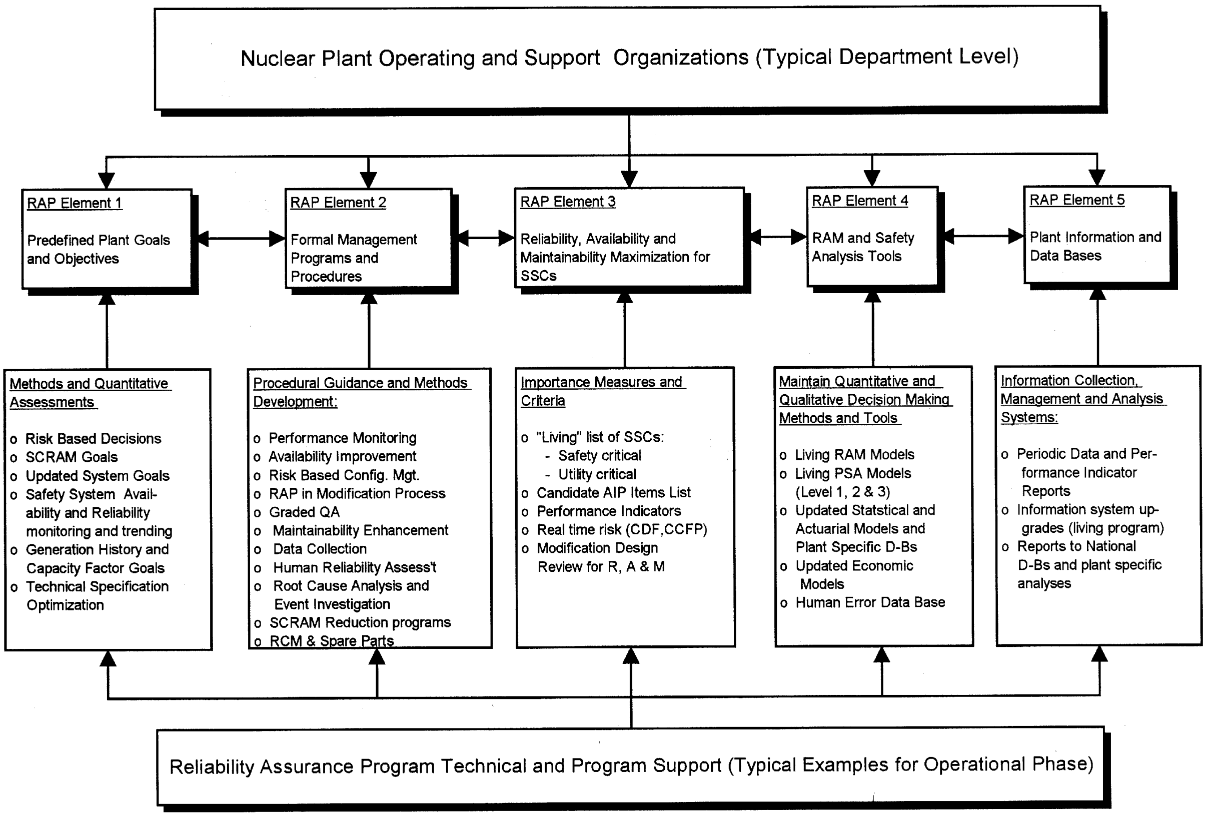

Nuclear Plant Operating and Support Organizations (Typical Department Level)
RAP Element 1
Predefined Plant Goals and Objectives
RAP Element 2
Formal Management Programs and Procedures
RAP Element 3
Reliability, Availability and Maintainability Maximization for SSCs
RAP Element 4
RAM and Safety Analysis Tools
RAP Element 5
Plant Information and Data Bases
Methods and Quantitative Assessments
o Risk Based Decisions
o SCRAM Goals
o Updated System Goals
o Safety System Availability and Reliability monitoring and trending
o Generation History and Capacity Factor Goals
o Technical Specification Optimization
Procedural Guidance and Methods Development:
o Performance Monitoring
o Availability Improvement
o Risk Based Config. Mgt.
o RAP in Modification Process
o Graded QA
o Maintainability Enhancement
o Data Collection
o Human Reliability Assess't
o Root Cause Analysis and Event Investigation
o SCRAM Reduction programs
o RCM & Spare Parts
Importance Measures and Criteria
o "Living" list of SSCs:
- Safety critical
- Utility critical
o Candidate AIP Items List
o Performance Indicators
o Real time risk (CDF,CCFP)
o Modification Design Review for R, A & M
Maintain Quantitative and Qualitative Decision Making Methods and Tools
o Living RAM Models
o Living PSA Models (Level 1, 2 & 3)
o Updated Statstical and Actuarial Models and Plant Specific D-Bs
o Updated Economic Models
o Human Error Data Base
Information Collection, Management and Analysis Systems:
o Periodic Data and Performance Indicator Reports
o Information system upgrades (living program)
o Reports to National D-Bs and plant specific analyses
Reliability Assurance Program Technical and Program Support (Typical Examples for Operational Phase)

*FIG. 7-2. O-RAP organizational interfaces.*

It is important to recognize the RAP does not generally change the need for existing plant programs, but, defines and applies a focused set of management processes with specific objectives which are aimed at enhancing the effectiveness of existing programs, and ultimately achieving the best plant life cycle performance that is possible.

An effective RAP organization will probably need a highly skilled group of specialists in RAM, PSA, reliability and maintainability engineering and data management and analysis which can provide the necessary technical support for each line organization whose activities can influence the reliability and availability of SSCs.

Because there is a need to examine issues which cross department or organizational lines, the RA program should have an interdepartmental forum to provide a high level arena where both technical and organizational issues can be discussed openly. Effective communication between plant organizations is essential to the long term success of RAP, so there will be an important need for a group of high level management representatives who can look beyond organizational lines and critically assess how well the plant-wide RA programs are working. The RAP oversight committee should meet these needs and objectives.

## Appendix

## DEFINITIONS USED IN RELIABILITY ASSURANCE

Four parameters are necessary to fully define the overall performance characteristics for a nuclear generating plant and each of its systems, structures and components (SSCs):

### Capability

The plant design, manufacture and construction must result in its having systems, structures and components which are capable of performing their intended functions under each specified set of operational boundary conditions, i.e. the plant is assured of being capable of generating electricity during all expected operational conditions and being capable of protecting the core, the reactor coolant system (RCS ) and containment following all expected plant upsets, transients and external threats.

### Efficiency

The plant must operate at an acceptable level of thermal efficiency while maintaining each of its intended functions. Because a nuclear plant has a thermal capacity (licensed reactor power), any reductions in efficiency will immediately appear as a reduction in plant output and as a reduction in plant capacity factor.

### Reliability

The plant must operate continuously at its full demanded load if it is to meet, or exceed, each of its prescribed economic goals. Any deviations from this state, either because SSC unreliability initiates a period of reduced output or an immediate reactor or turbine-generator trip, will result in an economic loss and, possibly, a challenge to the plant safety systems which in turn will have an incremental effect on plant risk and safety.

**Definition:** Reliability is defined as the probability that a specific hardware element, which is capable of meeting its intended function, will remain in an unfailed state for a specified period of time under a specified set of operational boundary conditions. SSC unreliability is commonly measured in terms of “mean time between failures” (MTBF) or its reciprocal, “failure Rate”.

Parameters used to measure the reliability of repairable components are as follows:
MTBF = Component-hours per period/component failures per period
Failure Rate = 1/MTBF

### Maintainability

Whenever the plant fails, either because it must operate at reduced output, or is completely shutdown, the economic penalty from lost generation becomes a function of how long it remains in that state, i.e. the time it takes to return the plant to complete functionality. This down time is determined by the plant “maintainability”.

**Definition**: Maintainability is a measure of the probability that a failed component can be restored to complete functionality within a specified period of time when under a specified set of operational boundary conditions. Mean down time (MDT) or mean time to repair (MTTR) are the operational parameters most often used to describe its effects.

Mean down time (MDT) can be defined as the mean time that a component remains in a fault or failed state before it is brought to an up state because of repair actions or inherent repair of the component.

Mean time to repair (MTTR) is analogous to MDT, but generally only includes only the mean time required to effect repairs, and does not necessarily include delays in failure discovery, administrative delays incurred when returning the component to service.

### Availability

Availability is a function both of how often the component fails (unreliability) and how long it takes to restore it to functionality after a failure (maintainability or down-time). When discussing a normally operating system, its availability becomes a measure which is related to its integrated capability (throughput or generation), when discussing a standby system, its availability is related to the probability that it will operate successfully on demand, i.e. be in a functional state at the time of demand.

**Definition**: Availability is defined as the probability that a component will be in a functional, or successful operating state, at any randomly selected future point in time.

Availability = MTBF/MTTR + MTBF
Unavailability = MTTR/MTTR + MTBF
If MTBF >>>MTRR
Unavailability $\simeq$ MTTR/MTBF

The reliability assurance program described by these guidelines provides a structured approach which will help to focus all plant institutional activities on maintaining an optimal level of reliability, maintainability and availability for each plant component, sub-system, system or functional success path. Rather than setting maximum levels of reliability or capacity factor or minimum risk as the goals for a reliability assurance program, an "optimum" level is sought wherever possible. This is because there is a point of diminishing returns for all reliability, availability and risk enhancement programs.

### Goal tree:

A logical and hierarchical functional structure which is derived deductively from a specified objective to show the interrelationships between objectives, functions and success paths.

### Success path:

A set of physical elements, which when they work in concert, provide an output which satisfies a particular functional objective.

**Institution**

An organizational infrastructure which implements specific programs and activities which influence the reliability, availability or maintainability of success paths.

**“Living” PRA plant model:**

A completed PRA is a "snapshot" in time of a plant's characteristics. Maintaining a living PRA requires that all changes be evaluated and, when applicable, incorporated into the PRA, since any change in the plant procedures and/or hardware has the potential to change the plant's characteristics and the PRA results. The living PRA provides a current model which can be used to evaluate the merit of potential changes or alternative operational strategies.

**A "risk-based inspection and testing" program**

Inspection and test programs are designed to examine passive components for any signs of deterioration of their capability and to test standby components to ensure their operability. Optimum scheduling of inspection and test intervals should be based upon the risk significance of potential failures of the components and upon the expected time interval between the appearance of early failure symptoms and the time at which the component will fail. Since passive components (such as a specific section of pipe) are often not included explicitly in a PRA, knowledge of this planned activity can result in the appropriate detail being built into the plant model

**Baseline risk profile and vulnerability assessment:**

The baseline assessment identifies the "as designed" or "as built" risk levels and provides a ranked list of the individual contributors. This ranked list of contributors becomes the starting point for a comprehensive risk reduction program whether in the design stage or post-construction.

**Condition monitoring analysis:**

The process of gathering information "on-line" for operating or standby hardware to provide an inference of internal condition or proper alignment can lead to real time assessments of failure propensities. The net benefit of these systems can be assessed with a risk model so that an estimate of their effectiveness can be established and the decision to install them made on a cost-justified basis.

**Integrated living schedule (ILS) or integrated management system (IMS):**

ILS/IMS is a process by which the implementation schedule for proposed facility changes is optimized on the basis of risk, within the normally present schedule and budgetary constraints.

**Life cycle costing:**

The process of allocating resources for facility improvements on the basis of their impact on lifetime facility costs. The plant models provide a mechanism for simulating the worth of the changes during the expected plant lifetime so that their integrated benefits can be estimated, and compared with the costs of their implementation. For example, the costing of various alternative process temperature control devices should include the liability risks that are associated with potential thermal runaway accidents.

**Man-machine interface:**

The role of the human is critical in the operation of all industrial facilities. A risk model can provide the necessary information on the "worth" of changes to this interface to ensure that resources expended to improve them are optimally expended.

**On-line process disturbance analysis and intelligent monitoring and alarming:**

Monitoring system parameters on-line may identify changes which are precursors to more significant events. A fault is diagnosed and provides forewarning to the operator so that preventive measures can be taken in time to mitigate an event which may become an "initiator". This type of system can also be used to diagnose system state during an upset so that direct event-specific recovery actions can be implemented by the operating staff, and limit the severity of the event. The cost effectiveness of the system can be established with the risk models.

**System interactions:**

The safety characteristics of a facility are often dominated by interactions between two or more seemingly independent systems. A risk assessment can identify coupling mechanisms and can provide a quantitative assessment of their importance. The assessment can then be used to evaluate the various proposed countermeasures and allow the identification of the most appropriate response.

**Applications involving normal operations**

The availability of models of the plant systems and knowledge of how operational procedures and maintenance policies affect system availability, plant availability, and public health and safety makes it easy and economical to do thorough studies of the implications of any proposed changes to the procedures and policies.

**Administrative policies/practices evaluation:**

Administrative policies/practices evaluation is a process by which the effects of proposed changes to the management and operation of a facility can be measured in terms of their impact on hardware and human performance, and their "worth" established a priori with a risk model.

**Availability improvement program:**

An availability improvement program is a structured examination of the productivity characteristics of a facility, in which a ranked list of contributors to unavailability is identified. This list becomes the starting point for an availability improvement process in much the same way as the facility baseline risk profile became the starting point for a risk reduction process.

**Performance analysis:**

Performance analysis is the process by which the individual events which occur in the operation of a facility can be simulated in the risk models to provide a high-level indication of facility performance. Performance indicators can be identified as surrogates for these detailed assessments.

**Reliability centered maintenance (RCM):**

RCM is a structured approach which identifies the important functional failure modes for plant hardware and the specific maintenance activities which can be implemented to prevent their unexpected occurrence. Risk models can provide both the prioritization for the examination of the individual hardware elements and the cost justification for any needed capital or operating expenses which result from the RCM analysis.

**Risk-based inspection and testing programs:**

A probabilistic risk assessment of a plant provides a basis for the prioritization of systems and components in terms of their risk importance. This can provide a rational basis for the scheduling of inspection and testing of those components and systems.

**Risk importance of operating events:**

To ensure that requisite resources are applied in the prevention of events which have risk significance, a risk assessment can provide direct estimates of the actual risk exposure from an experienced event. The magnitude of risk exposure for experienced events can then be used to prioritize the allocation of resources for a Corrective Actions program.

**Technical specification conformance and optimization:**

The technical specifications are designed to maintain the validity of the assumptions made in the facility safety analysis. It is economically important that they be no more restrictive than necessary, so risk assessments can be used to relax the requirements where appropriate. The duration of allowed safety equipment outage times and the frequency of required testings are defined by the technical specifications. These can be optimized with a risk assessment by ensuring that the requirements are modified to maximize the availability of individual hardware systems while maintaining an acceptably low level of risk.

## Annex

# 1. CASE STUDY # 1: PLANT RELIABILITY, AVAILABILITY AND MAINTAINABILITY (RAM) ANALYSIS FOR ADVANCED LIGHT WATER REACTOR (ALWR)

## 1.1. INTRODUCTION TO CASE STUDY # 1

The following case study was actually undertaken during the design and construction phase of an ALWR which will go into service in an IAEA member state in the near future. This study was designed to determine whether or not the plant could be expected to meet its prescribed performance goals. The study was also intended to produce a preliminary list of rank ordered SSCs which could be used to guide the development and implementation of an RCM programme. The study was based on the use of RAM analyses, both using analytical and actuarial bases, and is presented here because it both provides useful insights into the analytical process when there is very little plant-specific actuarial data available, and provides a good source of summary data for PWRs which can be used to benchmark future analyses.

In addition to the development of a RA programme by the NSSS vendor which primarily focused on the safety aspects of the design, a parallel study was to develop the rank-ordered list of safety related SSCs from the results of the plant specific PSA. These studies are beyond the scope of Case Study #1.

### 1.1.1. Overview of the ALWR RAM project objectives

The plant whose RAM analysis is described in this annex to the RAP guidebook is an ALWR which has the following general characteristics:

- 3800 MW•t pressurized water reactor with primary containment, designed to meet the general design criteria defined by the USNRC in 10CFR50 Appendix A,
- Integrated reactor-feedwater control system with automatic feedwater and reactor runback with turbine generator has fast valving so that on a load rejection, after the main generator breaker opens, the plant can quickly go to minimum unparalleled hotel loads and sustain the plant while isolated from the Electric Grid.

Other enhancements which influence the ALWR reliability and operability, when compared to similar plants of earlier plant designs, include:

- A digital feedwater control system,
- A deaerator in the feedwater system to provide some surge capacity,
- Increased redundancy in the condensate and feedwater trains and the absence of a pumped forward heater drain system,
- A reactor power cutback system and 100% turbine bypass capability.

### 1.1.2. Project objectives

The defined objectives for this RAM analysis were prescribed as follows:

- To identify each plant system which is important to overall plant unavailability and confirm that the current design is capable of meeting the specified plant level 80% availability goal,

- To identify each important plant component, system or subsystem whose failure will initiate a complete loss of plant capability (SCRAM or Shutdown) and to predict their associated frequencies,
- To calculate plant full forced outage rate by combining the frequencies and associated average plant down times for each identified Reactor SCRAM or shutdown scenario,
- To identify each dominant contributor to system and plant unavailability and wherever possible, propose cost effective measures to will reduce their individual importance,
- Review the results from the availability and reliability analyses and identify all "availability and reliability critical" components, subsystems or systems which should become candidates for inclusion in the plant RCM programme.

### 1.1.3. RAM project deliverables and analytical tasks

The project was structured to provide the following intermediate and final products:

- A coarse, plant level equivalent unavailability model which could be used to combine the results from each of the individual system availability models,
- A database which provided estimates of generic unavailability contributors in operating nuclear generating plants. This was used to provide initial guidance in selecting the systems which required detailed analysis,
- Individual system level equivalent unavailability models for systems which were expected to be important contributors to plant unavailability and an associated component level availability database,
- A critical components list with ranking on the basis of their individual contributions to unavailability,
- A component unreliability database and a plant level unreliability model which includes all systems and components whose failure will either
  - (i) Initiate direct reactor SCRAM,
  - (ii) Initiate turbine trip (and consequential reactor SCRAM),
  - (iii) Initiate turbine trip and operation on full turbine bypass,
- A critical components list with ranking on the basis of their individual contributions to unreliability (SCRAM frequency) and their associated plant mean down times,
- An estimate of the annual unavailability due to planned outages (annual planned maintenance and refueling outage),
- An estimate of the overall plant unavailability which uses all of the analytical results from the project to quantify the load duration curve,
- Identification of each potentially beneficial plant enhancements which could be a candidate for implementation, for example:
  - (a) Modifications which enhance hardware reliability or maintainability,
  - (b) Improved training, procedures or monitoring and diagnostic information which enhance the operators' ability to detect failures and take compensating actions in time to prevent a plant trip or shutdown,
  - (c) Critical components to be included in the RCM programme.
- Documentation of the RAM analyses and their results in a formal report.

Note:
In this study, fault tree analysis was used to calculate the frequency of plant SCRAMs, which is a measure of its unreliability, and the expected contributors to lost generation, a measure of its unreliability. Hence, throughout the study, unless they describe a particular methodology,

e.g. reliability block diagram analysis, the terms “unreliability” and “unavailability” are used to describe the construction of a specific type of failure oriented model.

## 1.2. TECHNICAL APPROACH

The plant unavailability modeling process progressed through the following stages and required the analytical RAM team to complete the following tasks:

- Develop a high level plant unavailability model which would facilitate the logical aggregation of the unavailability calculated from each individual system model,
- Construct functional diagrams (simplified P&IDs) for each modeled system, either by making a new drawing or marking up a set of plant P&IDs,
- Develop a set of simple reliability block diagrams for each modeled system included in the equivalent unavailability model. These diagrams showed the relationships between system success criteria and plant capability state so that they could be used to build the plant capability state matrix,
- Construct and quantify the plant availability fault trees with a fault tree analysis computer code. During construction and quantification of the unavailability fault tree models, the RAM team would:
  (a) Use a plant state matrix to define the discrete power state dependent failure criteria for systems included in the equivalent unavailability model,
  (b) Develop a documented, project-specific database for use as a standard basis for derivation of the basic event probabilities used in the quantification process
- Develop actuarial unreliability and unavailability models to augment the purposes. analytical models and to provide an experiential database which could be used for comparative.

### 1.2.1. Plant unreliability modeling

Development of the plant unreliability model processing moved through the following stages:

- Performance of a plant level failure modes and effects analysis (FMEA)

  A simplified high level failure modes and effects analysis was performed to document the analytical basis for assumptions made about the sources and effects of system and plant level failures and the assumptions to be made during construction of the fault tree. The FMEA also played an important role in providing the insights needed to identify each individual system which should be included in the project scope because they were expected to influence the reliability and availability of the plant.

- Definition of the fault tree top logic

  The top event for the unreliability model (fault tree) was defined as "complete loss of plant capability resulting from plant trip". The event was assumed to originate with either:
  (i) Reactor SCRAM caused by a process variable exceeding its protective action setpoint,
  (ii) Spurious reactor SCRAM caused by a fault in the reactor protection system hardware (sensors, logic, actuation, human error during maintenance and test) or loss of required protective system dependencies (AC, DC),
  (iii) Reactor SCRAM caused by actuation of ESFAS system (legitimate or spurious),

(iv) Turbine generator trip — initiated by a process variable exceeding its protective action setpoint,

(v) Spurious turbine tri -initiated by a fault in the turbine generator protective systems (sensors, logic, actuation, human error during test and maintenance) or loss of required support systems (AC, DC, cooling).

The high level logic for a typical unreliability model is shown in Figure A-1. This model shows how the ‘trip”model can be integrated with the manual trip and shutdown models for us in calculation of forced outage rates. If only SCRAM frequency is needed, the model is solved for the appropriate second level gate.

– Fault tree construction — scope and simplifications

During development of the unavailability and unreliability fault trees it was necessary to carefully maintain control over their boundaries to ensure that there was very little overlap between them to prevent double counting of individual contributions when the results from their analysis were used to calculate overall plant availability.

Industry data was used to determine the amount of detail included in the fault trees. Historically important causes of reactor SCRAM or shutdown were specifically addressed and the basic events in the tree were quantified with hourly failure rates taken from the component database.

– RAM analysis — application of the results

The results from the unavailability analysis provided an estimate of the failure probability for each plant state and a ranked list of important plant components and their associated unavailability. Each important contributor was then evaluated to determine whether it should be considered as a candidate for inclusion in the improvement programme and whether it should be specifically included in the plant RCM programme.

The results of the unreliability analysis were presented as ordered cutsets which provided the frequency and description of each scenario which could initiate an immediate plant shutdown. In aggregate, they provided an estimate of the expected rate for automatic and manually initiated "at power" SCRAMs and shutdowns:

(a) The positions of individual components in this ordered list became one of the criteria for their consideration for inclusion in the RCM programme,

(b) The mean down time (MDT) for each SCRAM was combined with its associated frequency of occurrence to provide an estimate of the plant unavailability contribution from full forced outages,

(c) The results from each individual analysis were combined to provide an overall estimate of the expected plant unavailability to confirm that the plant was capable of meeting the assigned performance goal of 80% availability,

(d) Where desirable changes were identified or required to ensure that the plant goal was met, cost benefit analyses were performed to ensure that the proposed changes were cost effective.

## 1.3. RAM METHODOLOGY DESCRIPTION AND ANALYTICAL GROUND RULES

### 1.3.1. Unavailability modeling

In the modeling of plant systems, it was not always necessary to include support systems within the infrastructure of the fault trees, as may be customary in PSA models:

(i) If the loss of a support system caused a plant trip or immediate shutdown it became part of the unreliability model. However the system fault events were moved to the top level of the fault tree. This approach was facilitated by the limited degree of true redundancy which exists among non-safety, power producing systems, and minimized the complexity in the model by leaving system fault tree models which contained only local (independent) faults,

(ii) If failure of a support system components lead to a long term plant reduction or shutdown, it was represented in a stand-alone support system unavailability model. This meant that each of the plant systems in the unavailability model could be treated independently and their individual unavailabilities summed to find the overall plant unavailability.

### 1.3.2. Unreliability modeling

Industry data which identified the historical causes of reactor SCRAM or shutdown was generally used to determine the level of detail needed in the unreliability fault trees. However, the analyst always retained the option to continue development beyond the suggested cut-off points whenever he thought it necessary to identify important support system dependencies, or if there was a suspicion that industry data did not apply:

– If the system or subsystem failure rate was less than 1 event in 1000 reactor-years, consideration was given to not developing the tree further,

– If the system or subsystem failure rate was between 0.01 and 0.001 per operating reactor-year, the fault tree was developed to the extent needed to confirm that the plant had no unique vulnerabilities.

In both of the above cases, it was confirmed that the plant design was similar or superior to other nuclear plants, before the decision was made to use data for an "undeveloped event" in lieu of detailed fault tree development:

– If the failure event rate was higher than 0.01 per operating reactor-year, development was generally continued to the component level.

The scope of the developed unreliability model was sufficient to represent all reactor and turbine trip functions which can initiate a plant automatic or manual SCRAM, although the guidelines defined above allowed some failures to be treated and quantified as undeveloped events.

Because the likelihood of having simultaneous independent failures in two out of four independent channels of ESFAS and RPS was expected to be negligible when compared with the likelihood of SCRAM caused by test and maintenance errors or failure of important support systems (HVAC, cabinet cooling, DC or instrument AC), the model was constructed to include only spurious actuations which resulted from:

- Loss of dependent systems,
- Test and maintenance test errors.

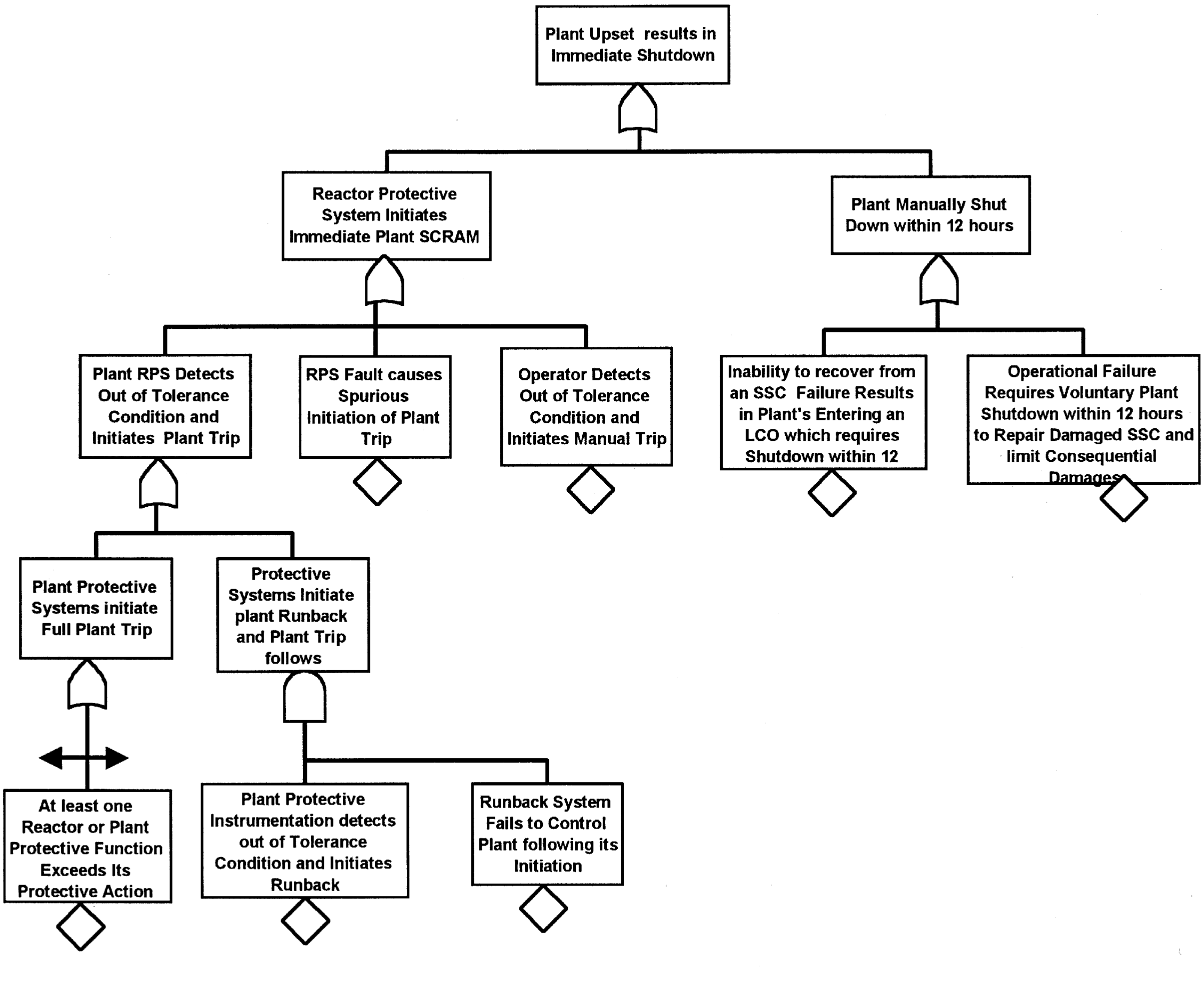
Because the turbine trip system could have "one out of two" or "two out of two" logic, decisions to limit model development were made on a case-by-case basis.

## 1.4. UNRELIABILITY ANALYSIS

A single fault tree was used to perform the plant unreliability analysis. The top event for this model was "immediate loss of plant capability initiated by automatic or manual shutdown", in which "immediate" meant within 12 hours (Figure A-1).

The secondary levels of the fault tree provided the opportunity to explore faults which initiated shutdown as a result of:

- Reactor SCRAM,
- Turbine/generator trip without a reactor SCRAM (to facilitate inclusion of the effects of failure of the power runback system),
- Manual shutdown.



Plant Upset results in Immediate Shutdown
Reactor Protective System Initiates Immediate Plant SCRAM
Plant Manually Shut Down within 12 hours
Plant RPS Detects Out of Tolerance Condition and Initiates Plant Trip
RPS Fault causes Spurious Initiation of Plant Trip
Operator Detects Out of Tolerance Condition and Initiates Manual Trip
Inability to recover from an SSC Failure Results in Plant's Entering an LCO which requires Shutdown within 12
Operational Failure Requires Voluntary Plant Shutdown within 12 hours to Repair Damaged SSC and limit Consequential Damages
Plant Protective Systems initiate Full Plant Trip
Protective Systems Initiate plant Runback and Plant Trip follows
At least one Reactor or Plant Protective Function Exceeds Its Protective Action
Plant Protective Instrumentation detects out of Tolerance Condition and Initiates Runback
Runback System Fails to Control Plant following its Initiation

*FIG. A-1. Reliability model — top logic.*

The fault tree was quantified with unreliability data taken from the project specific failure database, which provided an hourly estimate of trip frequency. This was later converted to its equivalent annual frequency.

The cutsets from the analysis provided a description of each scenario which would lead to initiation of a plant trip or immediate shutdown. Their individual rank, by order of occurrence frequency, generally provided their individual importance because quite a large number of them were single events.

## 1.5. UNAVAILABILITY ANALYSIS

The plant unavailability analysis was performed in two parts:

- An equivalent unavailability analysis (not shutdown),
- An operating unavailability analysis for plant systems which have a two-state mode of operation.

The results from each of these analyses were combined to provide an estimate of plant unavailability. A diagram showing each of the systems which constitute the plant wide unavailability model is shown in Fig. A-2 and the system functional model and its power dependent success criteria, needed to calculate equivalent unavailability, is shown in Fig. A-3.

The models were developed and solved as fault trees and quantified with data from the databases developed for the project. The cutsets from the analysis provided each of the plant component failure combinations which led to a reduction in capability or a controlled plant shutdown. These were ranked on the basis of their overall contribution to plant unavailability.

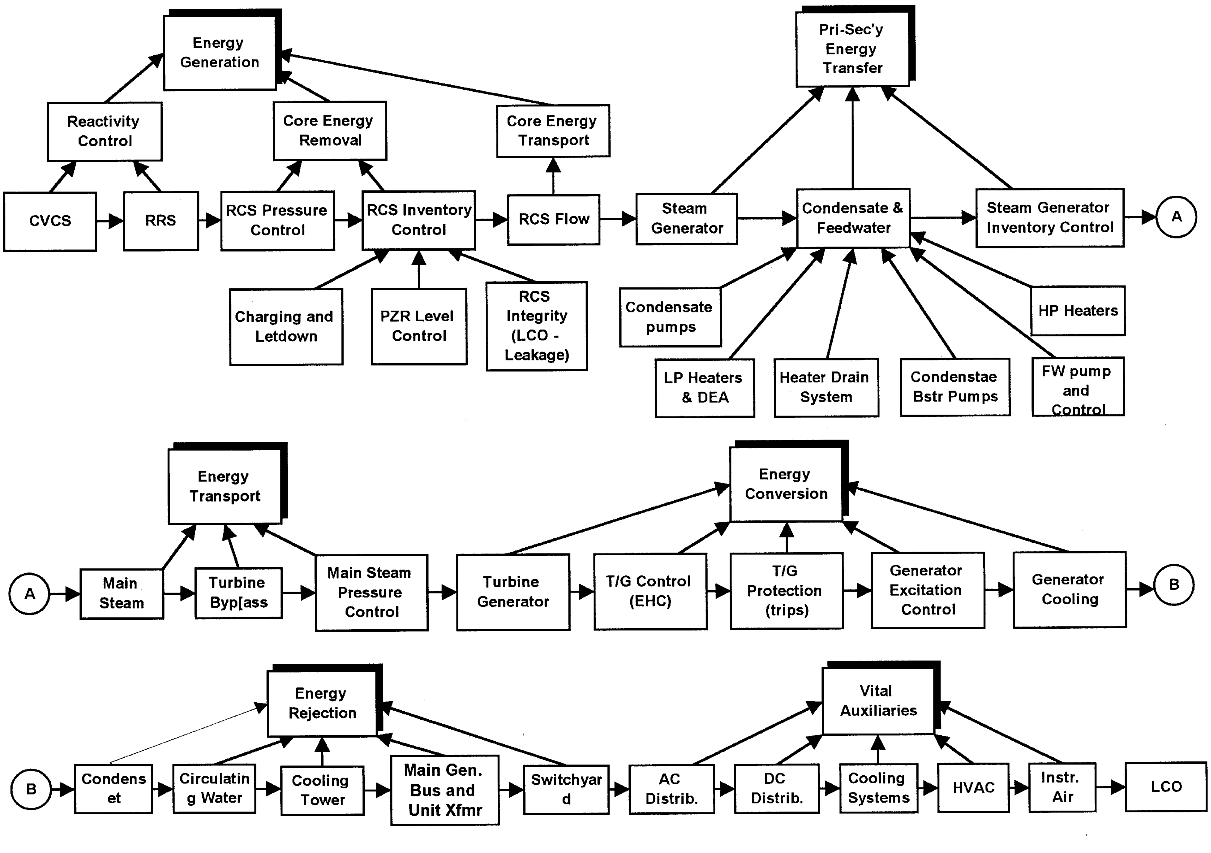
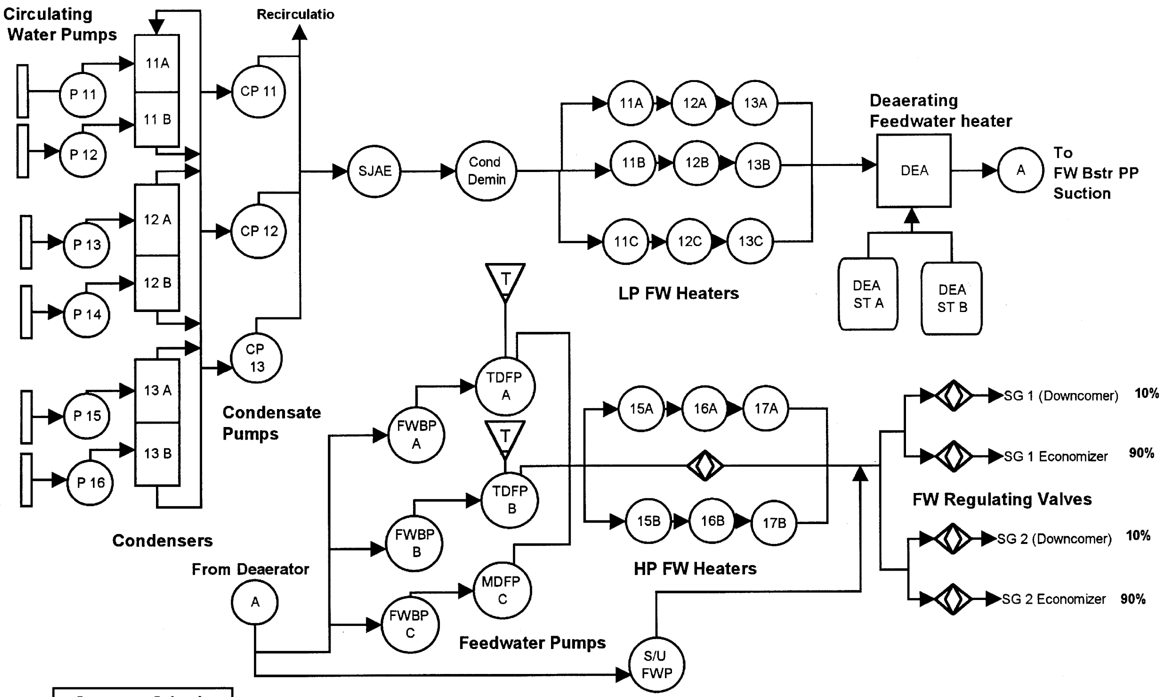


*FIG. A-2. Simplified availability model.*



**Success Criteria**

| Power | Condensers | Condensate Pps | LP Heaters | MFW Bstr Pumps | MFW Pumps | HP Heaters | FW Reg |
|---|---|---|---|---|---|---|---|
| 100% | 6 out of 6 | 2 out of 3 | 3 out of 3 | 2 out of 3 | 2 out of 3 | 2 out of 2 | Econ + DC (2 S/G) |
| 90% | 5 out of 6 | 2 out of 3 | 3 out of 3 | 2 out of 3 | 2 out of 3 | 2 out of 2 | 2 Econ + 2DC |
| 80% | 5 out of 6 | 2 out of 3 | 3 out of 3 | 2 out of 3 | 2 out of 3 | 2 out of 2 | 2 Econ + 2DC |
| 70 % | 5 out of 6 | 2 out of 3 | 3 out of 3 | 1 out of 3 | 1 out of 3 | 1 out of 2 | 2 Econ |
| 50% | 4 out of 6 | 1 out of 3 | 2 out of 3 | 1 out of 3 | 1 out of 3 | 1 out of 2 | 2 Econ |

*FIG. A-3. Condensate and feedwater system functional diagram.*

## 1.6. DATABASE

### 1.6.1 Plant specific database

A plant specific data for the plant was not available since it was under construction, however, an database was prepared from information collected throughout the operating lives of other indigenous nuclear plants. Review of this database showed, however, that there was insufficient detail for many SSCs and that the data did not encompass enough operating experience to allow its exclusive use as a result, the indigenous database was used to augment other sources of plant data which had been derived primarily from US plant experience.

### 1.6.2. Industry (generic) database

Two industry (generic) databases were prepared for the project:

- An initiating event (trip) database derived specifically for the type of plant from EPRI NP-2230 and NUREG/CR-3862. This database was used to guide the analyst in determining the appropriate level of fault tree detail during construction of the plant unreliability model (shown in Table A-I),
- A component specific unavailability database derived from a variety of international sources for operating failure rates and restoration times for the range of component types which were expected to be encountered during quantification of the unreliability and unavailability models.

The component unreliability and unavailability database was developed from information provided in a number of published databases (NERC-GADS, IAEA, EPRI). Expert judgement was used to augment the database where published information was not available. This was particularly true in identifying restoration times, since there is very little published data in this area.

TABLE A-I. SUMMARY OF HISTORICAL TRIP DATA FOR PLANTS SIMILAR TO THE ALWR

| Cat. | Transient Type | Ref. Plant Data (CR-3862) | Ref. Plant Data (EPRI) | NUREG/CR-3862 (PWR) | EPRI (All PWRs) | Indigenous Data |
|---|---|---|---|---|---|---|
| 1 | Loss of RCS flow–1 loop | 2E-1 | 8.5E-2 | 2.8E-1 | 4E-1 | |
| 2 | Uncontrolled Rod Withdrawal | NO OCC. | - | 1E-2 | 2E-2 | |
| 3 | CRDMs/Rod Drop | 5.5E-1 | 2.8E-1 | 5E-1 | 6.8E-1 | 3.9E-1 |
| 4 | Control Rod Leakage | 1.1E-1 | - | 2E-2 | 2E-2 | |
| 5 | Primary System Leakage | 4.5E-2 | 5.6E-2 | 5E-2 | 9E-2 | |
| 6 | High or Low PZR Pressure | NO OCC. | - | 3E-2 | 6E-2 | |
| 7 | Pressurizer Leakage | NO OCC. | - | 5E-3 | 1E-2 | |
| 8 | PORV/PSV Opening | 3E-2 | ? | 3E-2 | ? | |
| 9 | Inadvertent SIAS | NO OCC. | 4.2E-2 | 5E-2 | 6E-2 | |
| 10 | Containment Pressure | NO OCC. | - | 5E-3 | 1E-2 | |
| 11 | CVCS–Boron Dilution | 6E-2 | ? | 3E-2 | ? | |
| 12 | Press/Temp/Power Imbalance | 7.6E-2 | 5.6E-2 | 1.3E-1 | 1.7E-1 | |
| 13 | Start-up of Inactive RCP | NO OCC. | - | 2E-3 | 1E-2 | |
| 14 | Total loss of RCS Flow | 4.5E-2 | - | 3E-2 | 3E-2 | |
| 15 | Partial LOFW | 1.3E+0 | 2.8E-1 | 1.5E+0 | 1.8E+0 | 9.4E-1 |
| 16 | Total LOFW | 3.3E-1 | - | 1.6E-1 | 1.4E-1 | |
| 17 | Partial Closure MSIVs | 3E-2 | 7E-2 | 1.7E-1 | 2.6E-1 | |
| 18 | Closure of all MSIVs | 7.5E-2 | - | 4E-2 | 4E-2 | |
| 19 | Increase in FW (1 loop) | 2.1E-1 | - | 4.4E-1 | 6.8E-1 | |
| 20 | Increase in FW (all loops) | 3.2E-3 | - | 2E-2 | 2E-2 | |

| Cat. | Transient Type | Ref. Plant Data (CR-3862) | Ref. Plant Data (EPRI) | NUREG/CR-3862 (PWR) | EPRI (All PWRs) | Indigenous Data |
|---|---|---|---|---|---|---|
| 21 | FW Instability (OE) | 1.8E-1 | 1.4E-2 | 2.9E-1 | 1.5E-1 | |
| 22 | FW Instability (Mech.) | 1.4E-1 | 5.5E-1 | 3.4E-1 | 2.2E-1 | |
| 23 | Loss of Cond. Pp (1 loop) | 4.4E-2 | 2.8E-2 | 7E-2 | 9E-2 | 9.7E-2 |
| 24 | Loss of all Cond. Pps | NO OCC. | - | 1E-2 | 1E-2 | |
| 25 | Loss of Cond. Vacuum | 2E-1 | 4.2E-2 | 1.4E-1 | 2E-2 | |
| 26 | Steam Generator Leakage | 3E-2 (PAL) | 4.2E-2 | 3E-2 | 4E-2 | |
| 27 | Condenser Leakage | 3E-2 (PAL) | 1.4E-2 | 4E-2 | 5E-2 | |
| 28 | Sec'y System Leakage | 6E-2 | - | 9E-2 | 8E-2 | |
| 29 | Sudden opening — MSSVs | NO OCC. | - | 2E-2 | 5E-2 | |
| 30 | Loss of Circulating water | 6E-2 | 1.4E-2 | 5E-2 | 6E-2 | 1.4E-1 |
| 31 | Loss of CCW | 3E-2 | - | 2E-2 | - | 5E-2 |
| 32 | Loss of SRW | 3E-2 | - | 5E-3 | 1E-2 | |
| 33 | Turbine trip | 9E-1 | 2.8E-1 | 1.2E+0 | 3.8E-1 | 1.69E+0 |
| 34 | Generator Trip | 5.5E-1 | 1.4E-1 | 4.6E-1 | 1.4E-1 | 8.9E-1 |
| 35 | Loss of Station Power | 2.3E-1 | 4.2E-2 | 1.5E-1 | 1.4E-1 | 3.9E-1 |
| 36 | Pressurizer Spray failure | 1.5E-2 | 2.8E-2 | 3E-2 | 4E-2 | |
| 37 | Loss of Power to plant systems | 1.1E-1 | 3.4E-1 | 1.1E-1 | 9E-2 | 2.7E-1 |
| 38 | Spurious trip — cause unknown | 4.5E-2 | - | 8E-2 | 1.5E-1 | |
| 39 | Auto trip — no transient | 1.2E+0 | 5.6E-2 | 1.5E+0 | 1.6E+0 | |
| 40 | Manual Trip — no transient | 2.7E-1 | 8.5E-2 | 4.7E-1 | 6.2E-1 | |
| 41 | Fire within Plant | 3E-2 | - | 2E-2 | 3E-2 | |

## 1.7. METHODS AND CRITERIA USED TO REVIEW THE RESULTS

### 1.7.1. Identification of reliability critical components

Reliability critical components were identified directly from the ranked list of plant contributors described by the unreliability fault tree cut-sets or from the importance measures provided by the fault tree code.

### 1.7.2. Identification of availability critical components

Availability critical components were identified directly from the ranked list of plant contributors produced by the unavailability fault tree cut-sets or component importance measures provided by the fault tree code. This task could be performed directly with the results from the operating availability model, but the results from the equivalent availability model had to be treated more thoughtfully. because the equivalent unavailability analysis produced results for each plant capability state they had to be interpreted individually. If there was any doubt as to the importance of the unavailability contributions for specific components, sensitivity analyses were performed to provide additional insights about their "worth".

### 1.7.3. Identification of potentially important plant improvements

The list of important contributors to reliability and availability was used to prioritize the search for effective improvements. To identify potential improvements the analyst looked closely at each important contributor and determined whether:

- The component was an important contributor to plant unreliability or unavailability because it had high inherent levels of unreliability. If so, some of the improvement options were:
  (a) To be more selective in component procurement, i.e. specify reliability standards and purchase the most reliable component available,
  (b) To implement an effective reliability centered maintenance programme for that component (include it in the RCM programme),
  (c) To change the system design to increase its redundancy or diversity, i.e. reduce the impact of failures. In a multi-train, non redundant system, this may be achievable to some extent by increasing the capability of individual trains,
- The component was an important contributor to plant unavailability because it exhibited high average repair times. If so, some of the options were:
  (i) To minimize its failure rate, using the approaches identified above. This would reduce the plant’s exposure to the effects of SSC unavailability attributable to poor component maintainability,
  (ii) To perform a maintainability analysis which would ensure that the basic plant design and layout did not contribute to the problem more than it should.

  Maintainability analysis identifies the potential improvements in mean down time by remediating inadequacies in component assembly and disassembly requirements, laydown areas, personnel and equipment access, interference from other plant structures or components, inherent radiation protection for maintainers or poor environmental conditions (heat, light, ventilation).

– The component was an important contributor to unreliability or unavailability because of associated human errors. If so identified, some of the options open to the plant RAP design team could include:

  (a) Addition of improved diagnostic and monitoring instrumentation which will reduce the amount of testing and troubleshooting that a maintainer must do "on line",
  (b) Improvement in the information available to an operator so that he has more time available to respond to off-normal conditions,
  (c) Confirmation that the ergonomic interface between the operator and the plant is optimal in the areas in which the human error is perceived to originate (no error prone situations),
  (d) Procurement of components whose inherent maintainability characteristics minimize the likelihood of maintainer errors, i.e. simple assembly and disassembly.

As each important contributor was identified from the results of the analysis, it was evaluated in each general category described above to see if there were any remedial actions or beneficial changes which could be made. However, before any implementation recommendations could be made, the analyst had to consider other factors, in particular whether the proposed change was expected to be cost-effective.

### 1.7.4. Justification for proposed changes and improvements

All proposed changes to the plant, other than those which merely involve inclusion of a component or system in the RCM programme, should only be recommended when they can be shown to have a positive benefit cost ratio. Adding components to the RCM programme does not require justification because it has already been determined that such a programme will be implemented and all important components and systems will be included. The unavailability and unreliability analyses were only used to identify those components which were sufficiently unimportant that they could be excluded from the RCM programme.

### 1.7.5. Cost estimation

When the proposed change has been defined, the first step is to identify its cost. This cost must be found as a present worth of the life cycle costs. For example, if the change will result in additional costs which are incurred periodically throughout the life of the plant (increased maintenance or periodic component replacement) the periodicity and costs in the out-years must be converted to an equivalent present worth using the standard plant specific financial assumptions and techniques and added to the first cost.

### 1.7.5. Benefit estimation

To calculate the benefit from a proposed change, the plant models are modified to represent the "post-change condition" and new results obtained. The difference between the original "baseline" unavailability contribution and the new, post modification unavailability represents the benefit, which is then converted to an equivalent increase in generation.

The benefit from increased generation and plant capacity from the change, throughout the life of the plant, must also be converted to an equivalent present worth using standard financial assumptions for the plant so that it is on the same basis as the cost estimate and can be compared directly with the cost.

### 1.7.6. Cost–benefit ratio

When the benefit–cost ratio has been calculated for a specific change, the following criteria can be used to guide the analyst in deciding upon the strength of the recommendation for its implementation:

- If the benefit-cost ratio >3, then **recommend** implementation,
- If 1 < benefit-cost ratio <3, then **consider** implementation, but first, look at other factors which may influence the decision (total cost, uncertainty, schedule impact, etc.),
- If the benefit-cost ratio <1 , then **do not recommend** implementation.

The use of a factor of three to measure the strength of the recommendation is derived from an insight that the normal error factor associated with analyses of this type has a value of three. By using a positive cost benefit measure of three to trigger the recommendation for implementation, the normal degree of uncertainty is accommodated without having to perform a detailed uncertainty analysis. If the modification involves a significant capital outlay or could have an impact on project schedule, a more detailed assessment would normally be performed to determine whether the uncertainty of more or less than assumed by this rule of thumb, and whether it changes the decision.

It is important to recognize that the techniques being discussed are used as decision making aids. Increasing amounts of accuracy (or decreasing uncertainty) are only important if they have the potential to affect the outcome of the decision making process.

## 1.8. PLANT UNRELIABILITY ANALYSIS

### 1.8.1. Fault tree top logic

The plant unreliability analysis was performed with the development and solution of a single fault tree whose top event was "immediate loss of plant capability initiated by automatic or manual shutdown". The simplified FMEA, shown in Table A-II was used to document and confirm the assumptions made during development of the fault tree logic, particularly in the areas of completeness. Ensuring that each important contributing component or system failure was included in the models was of utmost importance.

The second level of the fault tree provided the opportunity to explore faults which initiated shutdown as a result of:

- Reactor SCRAM,
- Turbine/generator trip without a reactor SCRAM (to accommodate failure of the power runback system),
- Manual shutdown.

Note:
Immediate plant shutdown was defined to include all shutdown events which culminated in a plant shutdown within 24 hours.

TABLE A-II. INITIAL ASSESSMENT OF THE POSSIBLE EFFECTS FROM SYSTEM FAILURES (FUNCTIONAL FMEA)

| Plant Function | Plant System | System Failure Initiates plant FO | Effect of failure on the plant |
|---|---|---|---|
| Energy Generation | Reactor Protection | yes | Immediate plant trip |
| | Engineered Safeguards | yes | Actuation of SIAS or SDS initiates a plant trip |
| | CVCS (reactivity) | possible | Inadvertant boron dilution could initiate HI POWER trip if it happens fast enough — time of life likely important<br>Inadvertant boron addition — power decrease, LO DNBR or LOW PZR pressure if turbine is not runback to match primary power |
| | RRS (Reactivity) | yes | Inadvertant rod withdrawal will initiate HI POWER Trip<br>Improper rod position will initiate HI LOCAL Power trip<br>Dropped rod may initiate trip on LO DNBR or LOW PZR Pressure if turbine runback does not occur |
| | CVCS (RCS Inventory control) | yes | Loss of charging — Low DNBR or LOW PZR Pressure<br>(charging pumps, VCT valves)<br>Isolation of Letdown — HI PZR pressure<br>(Letdown valves) |
| | RCS Pressure control | yes | PZR heaters — stay on — HI PZR pressure<br>Excessive Sprays — LO DNBR/LO PZR pressure |
| | RCS Inventory control | yes | Reduction in Charging — LOW DNBR or LOW PZR Pressure<br>Reduction in Letdown — HI PZR pressure |
| | RCS Flow | yes | RCP trip (breaker, loss of 13Kv)<br>LOW RCS Flow |
| Energy Transfer | Steam Generator (tubes) | yes | HI SG Level, HI SG Pressure |
| | Steam generator Blowdown system | possible | Failure to reclose the valves in the SGBS may initiate LOW SG Pressure |
| Energy | Condensate and | yes | Reduction in FW Flow can lead to LOW SG |

| Plant Function | Plant System | System Failure Initiates plant FO | Effect of failure on the plant |
|---|---|---|---|
| Transfer (feedwater inventory) | Feedwater | | LEVEL |
| | Steam generator level control | yes | LOW SG Level<br>HIGH SG Level<br>(Depends upon the nature of the fault -<br>Closure of any FW regulating valves will likely initiate LOW SG Level) |
| Energy Transport (Steam) | Main Steam (Flow isolation) | yes | Closure of the MSIVs will initiate HI SG Level and HI PZR Pressure |
| | Turbine Bypass/Atmospheric Dump valves | yes | If the TBVs Fail open they will initiate LO SG Pressure.<br>Failure of the Power Cutback System (PCS) or the TBS following a turbine trip will initiate HI PZR Pressure |
| | | | |
| Energy Conversion | Turbine/Generator | possible | Turbine-Generator failure will actuate T-G trip, which in turn will initiate HI PZR pressure if TBS or PCS do not function properly on demand |
| | Turbine/Generator Protection | possible | T-G trip will initiate HI PZR pressure if TBS or PCS do not function properly on demand |
| | Generator/exciter | | T-G trip will initiate HI PZR pressure if TBS or PCS do not function properly on demand |
| | Generator cooling | | Failure of generator cooling will initiate turbine generator trip |
| | Turbine/Generator control | | Loss of control will initiate<br>Power-load imbalance T-G trip |
| Energy Rejection | Condenser | Likely if catastro-phic | Condenser failure will initiate high conductivity (or high sodium) in the condensate system and lead to a reduction in load when the condenser is removed from service. Catastrophic failure will lead to manual plant trip to prevent contamination of the SGs |
| | Condenser Vacuum | yes | Loss of condenser vacuum will initiate FW pump trip (Turbine backpressure) and LOW SG Level. Turbine trip will also be initiated.<br>If operating on the MDFW Pump, TBS will not actuate on turbine trip, so RPS will trip on HI PZR Pressure |

| Plant Function | Plant System | System Failure Initiates plant FO | Effect of failure on the plant |
|---|---|---|---|
| | Condenser inventory Spill/make-up | yes | Loss of condenser level will initiate a condensate pump trip and loss of feedwater — trip on LOW SG level |
| | Circulating water system | | Circulating water system failure will initiate loss of condenser vacuum |
| Energy Transport (electric) | Main generator buses & Bkrs | | Loss of load trip for T-G |
| | Bus duct cooling | | Generator trip (or manual load reduction and shutdown) |
| | Unit Transformer(s) | | Loss of load trip of the T-G |
| | Switchyard | yes | Potential loss of offsite power and RPS trip — LOW RCS Flow.<br>Loss-of-Load turbine trip |
| Vital Auxiliaries | AC Distrib. (13Kv, 4Kv, 480v) | yes | 13Kv - Loss of RCPs — LOW RCS Flow<br>4Kv - Loss of Condensate and booster pumps — LOW SG Level<br>480v - ? |
| | DC Distrib. (125vdc, 250vdc) | probable | 125vdc -loss of DC to FW pump speed controllers and loss of FW — LOW SG Level (?) |
| | Instrument AC | probable | Loss of control power will likely lead to a turbine or feedwater trip but a specific evaluation will have to be made — the outcome may depend upon the failure mode for control components (Fail high, or actuate when de-energized)<br>If the condensate and feedpump minimum flow valves fail open when deenergized, loss of feedwater will result |
| | Component Cooling Water | likely | Loss of RCP seal cooling, RCP trip and LOW RCS Flow<br>Loss of CEDM cooling<br>Loss of charging pump cooling<br>Loss of containment cooling (essential and containment building chillers) |
| | Service Water | likely | Loss of component cooling |

| Plant Function | Plant System | System Failure Initiates plant FO | Effect of failure on the plant |
|---|---|---|---|
| | Turbine Bldg CCW | yes | Loss of Lube Oil cooling for turbine, condensate and feedwater pumps, Turbine trip, Loss of Feedwater, LO SG Level |
| | HVAC -Turb. Bldg | | |
| | HVAC — SWGR Rooms | | Potential loss of 13Kv, 4KV and 480vac |
| | HVAC — control room, computer room or cable spreading room | possible | Excessive temperature may initiate ESFAS actuation of SDS (Palo Verde)<br>Core power programmemers may fail and initiate dropped rods<br>RPS trip is possible (manual), |
| | Instrument Air | | Non determinate without examination of the effects of loss of instrument air on individual valves e.g. loss of IA may cause condensate and feedwater minimum flow valves to fail open with a subsequent loss of feedwater. |
| Regulatory (LCOs) | | | Generally will lead to a controlled shutdown, not a plant trip (availability, not reliability issue) |

The general structure of the fault tree at the next, and each succeeding level provided identification of faults which caused a shutdown for the following reasons:

- Process parameters exceeded their protective action thresholds (trip setpoints),
- Spurious actuation of protective functions were caused by either:
  (i) Hardware failures within the protective systems,
  (ii) Inadvertent actuation of the protective systems as a result of human error (test and maintenance),
  (iii) Failure of support systems which cause actuation of the protective systems (120vac, 125vdc, 250vdc, etc.).

Each individual trip function was identified and included in the lower levels of the fault tree and developed to the point the origins of process system and support system faults which initiate protective system actuation could be identified.

### 1.8.2. Modeling limitations and simplifications

In some cases, where support system failures were found to always result in a reactor or turbine/generator trip, they were elevated within the tree as stand alone models rather than remaining in their normal hierarchal position in the tree structure. This was done to reduce model complexity and allow most of the system models to be represented as a set of local faults.

## 1.9. PLANT UNAVAILABILITY ANALYSIS

### 1.9.1. Plant unavailability block diagram

The plant unavailability analysis was performed in two parts:

(1) An equivalent unavailability analysis was performed for those plant systems which are capable of operating in a degraded mode which results in reduced plant capability but not shutdown,

(2) An operating unavailability analysis was performed for plant systems which have a two-state mode of operation, i.e. if the system is available, plant capability is unaffected, if the system is unavailable, the plant must be shut down.

Combination of the results from each of these analyses allowed estimation of plant unavailability. A diagram showing each of the systems which constitute the plant wide unavailability model is shown in Fig. A-2.

### 1.9.2. Equivalent unavailability analysis and the plant state matrix

- Systems in the flow path from the plant heat sink (circulating water) to the steam generator form the basis for the equivalent unavailability model,
- The plant capability states of interest were defined to provide enough points from which to develop the equivalent unavailability curve, i.e. 100%, 90%, 85%, 80%, 75% and 70%.

### 1.9.3. Fault tree development for the equivalent unavailability analysis

The plant model was developed as a series of fault trees, each of which had plant state capability failure criteria specific to its logic.

The success/failure criteria for each of these states was determined directly from the functional block diagram shown in Figure A-3 and defined by the variable success criteria in the capability state matrix, also shown in the lower section of Fig. A-3. The unavailability for each event in the fault tree was quantified from the operating failure rates and restoration times provided in the Reliability and Availability database.

### 1.9.4. Operating unavailability analysis

#### Plant unavailability block diagram

Systems which are shown in the overall plant availability model, Fig. A-2, but which were excluded from the equivalent unavailability model shown in Fig. A-3, become part of this model. A small fault tree, which includes all of its major components, is developed for each system. These individual system fault trees are then merged under a single OR gate to represent the complete plant unavailability model.

## 1.10. SYSTEM AND COMPONENT FAILURE DATA BASES

### 1.10.1. Plant specific component level database

A database was compiled from information reported by indigenous plants, but, because of the sparseness and lack of specificity at the component level, the models were initially quantified from the generic database compiled from a range of sources, specifically for this project. Later, where it was warranted, detailed plant specific data was compiled for individual components.

The plant PSA data was well developed at the time that the analysis was initiated, however its scope did not embrace the necessary range of "balance of plant" components, neither did it include repair times, a very important needed attribute for the database used to perform the availability analysis.

### 1.10.2. Initiating event and reactor trip databases

To identify those elements of the reliability model which could be abbreviated, a comparison was made between the histories of initiating event frequencies for plants with similar operating conditions, generic industry and specific experience for plants with similar construction. Industry data was drawn from EPRI NP-2230 and NUREG/CR-3862. The results of this comparison are shown in Table A-I.

Following the system level FMEA shown in Table A-II, several tables are provided to describe the operating history for all US nuclear plants for the ten year period from 1976 through 1985:

- Table A-III: Unavailability for US Nuclear Plant Systems (NERC-GADS Data, All Nuclear Plants 1975 thru 1985),
- Table A-IV: Forced Reductions for Nuclear Plant Systems (NERC-GADS Data, All US Nuclear Plants 1976 thru 1985),
- Table A-V: Indigenous National Experience with Nuclear Plant Forced Outages.

In addition to the above data analysis, a summary table of indigenous national experience was also performed and is shown in Table A-V, below.

TABLE A-III. UNAVAILABILITY FOR US NUCLEAR PLANT SYSTEMS (NERC-GADS DATA, ALL NUCLEAR PLANTS 1975 THRU 1985)

| Rank: Rel/Avail | System | Avg. FO Frequency All plants 1976–85 | Avg. FO Hours/year All plants 1976–85 |
|---|---|---|---|
| 3/2 | Steam Generators | 0.62 | 121 |
| 7/7 | RCS Valves and piping | 0.29 | 47 |
| 5/6 | RCPs and Recirc. Pumps | 0.44 | 56 |
| 9/4 | Misc. NSSS | 0.24 | 65 |
| 17/17 | CCW | 0.03 | 4 |
| 15/15 | CVCS | 0.05 | 6 |
| 7/8 | Control Rods & Drives | 0.29 | 31 |
| 16/16 | Pressurizer | 0.04 | 5 |
| 12/11 | Safety System Valves & piping | 0.14 | 12 |
| 12/11 | Containment & HVAC | 0.12 | 12 |
| 10/13 | Reactor Control — I&C | 0.18 | 8 |
| 4/10 | Reactor Protect. — I&C | 0.46 | 17 |
| 11/13 | Nucl. Instr. | 0.15 | 8 |
| 13/17 | Eng'g Safeguards — I&C | 0.11 | 4 |
| 16/19 | Aux. Systems — I&C | 0.04 | 1 |
| 12/18 | Control and Instrument Power | 0.14 | 3 |
| 2/3 | Turbine | Mech. –0.6<br>Control– 0.1<br>Misc. –0.1<br>Total –0.8 | Mech. -<br>84<br>Control -<br>13<br>Misc. -<br>3<br>Total -<br>10<br>0 |

| Rank: Rel/Avail | System | Avg. FO Frequency All plants 1976–85 | Avg. FO Hours/year All plants 1976–85 |
|---|---|---|---|
| 6/5 | Generator | Mech. –0.02<br>Electr. -0.06<br>Control -0.22<br>Cooling –0.06<br>Misc. - 0.06<br>Total - 0.36 | Mech. - 2<br>Electr. - 30<br>Control - 12<br>Cooling - 9<br>Misc. - 7<br>Total - 60 |
| 12/7 | MS/R | 0.14 | 4 |
| 1/7 | Feedwater | PPs.& Drives - 0.26<br>FW Valves - 0.25<br>Heaters– 0.06<br>Other – 0.35<br>Total - 0.92 | Pumps&Drives– 8<br>FW valves– 7<br>Heaters – 3<br>Other – 29<br>Total - 47 |
| 17/19 | Condensate Pumps | 0.03 | 1 |
| 12/14 | Condenser | Tubes - 0.07<br>Leaks & Vac. - 0.07<br>Total - 0.14 | Tubes – 4<br>Leaks & Vac– 3<br>Total – 7 |
| 17/18 | Circulating water PPs. | 0.03 | 3 |
| 18/20 | TBCCW | 0.00 | 0.15 |
| 8/9 | Maintenance errors | 0.25 | 21 |
| 14/12 | Main Transformer | 0.07 | 10 |
| 18/19 | Auxiliary Transformer | 0.00 | 1 |
| 14/17 | Switchgear | 0.07 | 4 |

| Rank: Rel/Avail | System | Avg. FO Frequency All plants 1976–85 | Avg. FO Hours/year All plants 1976–85 |
|---|---|---|---|
| | Sub-Total | 6.2 | 661 |
| 1/1 | Safety Problems - Admin. or Regulatory | 0.1 | 126 |
| | Total | 6.3 | 787 (10%) |

TABLE A-IV. FORCED REDUCTIONS FOR NUCLEAR PLANT SYSTEMS (NERC-GADS DATA, ALL US NUCLEAR PLANTS 1976 THRU 1985)

| Rank | System | FR Frequency — All plants 1976–85 | Avg. Equiv Hours/year 1976–85 |
|---|---|---|---|
| 5. | Steam Generators | 1.2 | 14 |
| 14. | RCS Valves and piping | 0.2 | 1 |
| 6. | RCPs and Recirc. Pumps | 1.1 | 11 |
| 2. | Misc. NSSS | 5.1 | 20 |
| 17. | CCW | 0.1 | 0.1 |
| 14. | CVCS | 0.2 | 1 |
| 11. | Control Rods & Drives | 0.6 | 3 |
| 20. | Pressurizer | 0.1 | 0.04 |
| 14. | Safety System Valves & piping | 0.1 | 1 |
| 15. | Containment & HVAC | 0.1 | 0.7 |
| 15. | Reactor Control — I&C | 0.2 | 0.7 |
| 15. | Reactor Protect. — I&C | 0.2 | 0.7 |
| 13. | Nucl. Instr. | 0.3 | 1.3 |
| 17. | Eng'g Safeguards — I&C | 0.04 | 0.1 |
| 18. | Aux. Systems — I&C | 0.01 | 0.06 |
| 19. | Control and Instrument Power | 0.05 | 0.05 |
| 3. | Turbine | Mech. –1.0<br>Control– 0.8<br>Misc. –0.5<br>Total –2.3 | Mech. - 14<br>Control - 2<br>Misc. -3<br>Total -19 |

| Rank | System | FR Frequency — All plants 1976–85 | Avg. Equiv Hours/year 1976–85 |
|---|---|---|---|
| 8. | Generator | Mech.– 0.01<br>Electr.– 0.15<br>Control– 0.12<br>Cooling - 0.12<br>Misc.– 0.07<br>Total– 0.47 | Mech. -0.12<br>Electr. -0.57<br>Control -0.22<br>Cooling -3.3<br>Misc. -0.3<br>Total - 4.5 |
| 10. | MS/R | 0.5 | 3.3 |
| 1. | Feedwater | PPs.& Drives– 1.26<br>FW Valves - 0.14<br>Heaters– 0.66<br>Other –3.9<br>Total– 6.0 | Pumps&Drive s- 7<br>FW valves– 0.7<br>Heaters –5.3<br>Other –21.5<br>Total –34.5 |
| 9. | Condensate Pumps | 0.5 | 4 |
| 4. | Condenser | Tubes - 3.4<br>Leaks & Vac.– 0.2<br>Total– 3.6 | Tubes -15<br>Leaks & Vac - 1.4<br>Total -16.4 |
| 12. | Circulating water PPs. | 0.4 | 2.2 |
| 20. | TBCCW | 0.01 | 0.04 |
| 17. | Maintenance errors | 0.05 | 0.1 |
| 16. | Main Transformer | 0.07 | 0.3 |
| 17. | Auxiliary Transformer | 0.01 | 0.1 |
| 17. | Switchgear | 0.04 | 0.1 |
|  | Sub-Total | 24.4 | 138 (1.6%) |
| 7. | Safety Problems - Admin. or Regulatory | 0.84 | 8 |
|  | Total | 25.2 | 146 (1.7%) |

TABLE A-V. NATIONAL EXPERIENCE WITH NUCLEAR PLANT FORCED OUTAGES

| Origin of Forced Outage | FO Frequency | Avg. FO<br>h/a | Importance |
|---|---|---|---|
| Generator | 0.53 | 168 | Very High |
| Reactor Coolant System | 0.31 | 41 | High |
| Feedwater | 0.96 | 37 | High |
| Main Turbine | 0.75 | 35 | High |
| Main power<br>(Generator to System) | 0.36 | 26 | High |
| CEDMs | 0.38 | 17 | Mod-High |
| Reactor Protective System | 0.26 | 15 | Mod-High |
| Offsite Power | 0.29 | 10 | Moderate |
| Incore Nuclear Instrumentation | 0.025 | 9 | Moderate |
| Main Steam | 0.46 | 7 | Moderate |
| Extraction Steam | 0.05 | 7 | Moderate |
| Circulating water | 0.14 | 5 | Low |
| Component Cooling water | 0.05 | 5 | Low |
| Instrument and Control Power | 0.17 | 3 | Low |
| Switchyard | 0.1 | 3 | Low |
| DC Power | 0.1 | 3 | Low |
| Condensate | 0.1 | 2 | Low |
| Instrument Air | 0.05 | 1 | Very Low |
| TBOCWS | 0.02 | 0.5 | Very Low |

TABLE A-VI. IMPORTANT SYSTEMS LIST

| System | Importance to Reliability | Importance to Availability |
|---|---|---|
| Feedwater System -Pumps<br>- FW Regulating<br>- Heaters | Very High<br>Very High<br>Low | Very High<br>High<br>High |
| Condensate system- Cond. Pumps<br>- Condenser | Very Low<br>Low | Low<br>High |
| Turbine | Very High | Very High |
| Generator | High | Very High |
| Steam generators | Very High | Very High |
| Reactor Coolant pumps | Very High | Very high |
| RCS valves and piping | High | High |
| Reactor Protection — I&C | Very high | Moderate |
| Control Rods, Drives and Reactor Control | Very High | Moderate |
| Nuclear Instrumentation | Moderate | Low |
| Control and Instrument Power | Moderate | Low |
| Containment and Containment HVAC | Moderate | Low |
| Engineered safeguards | Moderate | Low |
| Auxiliary Systems — I&C | Low | Very Low |
| Circulating Water — pumps | Very Low | Low |
| CVCS | Low | Low |
| Component Cooling Water | Low | Low |
| Service Water | low | Low |
| MSIVs | Low | Low |
| Main Transformer | Low | Low |
| Auxiliary Transformer | Very Low | Very low |
| Switchgear | Very Low | Very low |
| Turbine Building Closed Cooling Water | Extremely low | Extremely Low |

In addition to the systems above, the issue of administrative and regulatory shutdowns should be considered on the same scale:

| System | Importance to Reliability | Importance to Availability |
|---|---|---|
| Regulatory and administrative shutdown | Low | Very High |

No other plant systems appeared in the data for trips, transient initiators or unavailability. This list was compared with and generally found to be consistent with forced outage contributions from indigenous plant failures shown in Table A-V.

In an attempt to determine the extent to which the historical trip data for a reference plant is applicable "as is" to the ALWR design, two additional analyses were performed. Table A-VII represents data taken from NUREG/CR-3862 for plants similar to the reference plant, but excludes the performance of the two oldest plants and the first year of operation for each of the others: Table A-VII.

The last data assessment to be performed in order to better understand the trip frequency which could be expected for a plant built to today's standards, involved review of the trip frequency data for similar plants to identify any trend which can be attributed to factors other than design.

Table A-VIII: History of Reactor Trips for Units in the USA which are comparable to the reference plant

TABLE A-VII. SUMMARY OF HISTORICAL TRIP DATA

| Cat | Transient Type | Reference Plant Design Data (CR-3862) | Limited Reference Plant data | Reference Plant Data (EPRI) | NUREG/ CR-3862 | Indigenous Data |
|---|---|---|---|---|---|---|
| 1 | Loss of RCS flow — 1 loop | 2E-1 | 2E-1 | 8.5E-2 | 2.8E-1 | |
| 2 | Uncontrolled Rod Withdrawal | NO OCC. | NO OCC. | - | 1E-2 | |
| 3 | CRDMs/Rod Drop | 5.5E-1 | 3E-1 | 2.8E-1 | 5E-1 | 3.9E-1 |
| 4 | Control Rod Leakage | 1.1E-1 | NO OCC. | - | 2E-2 | |
| 5 | Primary System Leakage | 4.5E-2 | 7.3E-2 | 5.6E-2 | 5E-2 | |
| 6 | High or Low PZR Pressure | NO OCC. | NO OCC. | - | 3E-2 | |
| 7 | Pressurizer Leakage | NO OCC. | NO OCC. | - | 5E-3 | |
| 8 | PORV/PSV Opening | 3E-2 | NO OCC | ? | 3E-2 | |
| 9 | Inadvertent SIAS | NO OCC. | NO OCC | 4.2E-2 | 5E-2 | |
| 10 | Containment Pressure | NO OCC. | NO OCC | - | 5E-3 | |

| Cat | Transient Type | Reference Plant Design Data (CR-3862) | Limited Reference Plant data | Reference Plant Data (EPRI) | NUREG/ CR-3862 | Indigenous Data |
|---|---|---|---|---|---|---|
| 11 | CVCS — Boron Dilution | 6E-2 | 5E-2 | ? | 3E-2 | |
| 12 | Press/Temp/Power Imbalance | 7.6E-2 | 1E-1 | 5.6E-2 | 1.3E-1 | |
| 13 | Start-up of Inactive RCP | NO OCC. | NO OCC. | - | 2E-3 | |
| 14 | Total loss of RCS Flow | 4.5E-2 | 2.4E-2 | - | 3E-2 | |
| 15 | Partial LOFW | 1.3E+0 | 1.0E+0 | 2.8E-1 | 1.5E+0 | 9.4E-1 |
| 16 | Total LOFW | 3.3E-1 | 3.6E-1 | - | 1.6E-1 | |
| 17 | Partial Closure MSIVs | 3E-2 | 5E-2 | 7E-2 | 1.7E-1 | |
| 18 | Closure of all MSIVs | 7.5E-2 | 2.4E-2 | - | 4E-2 | |
| 19 | Increase in FW (1 loop) | 2.1E-1 | 2.2E-1 | - | 4.4E-1 | |
| 20 | Increase in FW (all loops) | 3.2E-3 | 2.4E-2 | - | 2E-2 | |
| 21 | FW Instability (OE) | 1.8E-1 | 2.0E-1 | 1.4E-2 | 2.9E-1 | |
| 22 | FW Instability (Mech.) | 1.4E-1 | 1.2E-1 | 5.5E-1 | 3.4E-1 | |
| 23 | Loss of Cond. Pp (1 loop) | 4.4E-2 | 5E-2 | 2.8E-2 | 7E-2 | 9.7E-2 |
| 24 | Loss of all Cond. Pps | NO OCC. | NO OCC. | - | 1E-2 | |
| 25 | Loss of Cond. Vacuum | 2E-1 | 1.E-1 | 4.2E-2 | 1.4E-1 | |
| 26 | Steam Generator Leakage | 3E-2<br>(PAL) | NO OCC. | 4.2E-2 | 3E-2 | |
| 27 | Condenser Leakage | 3E-2<br>(PAL) | NO OCC. | 1.4E-2 | 4E-2 | |
| 28 | Sec'y System Leakage | 6E-2 | 7.3E-2 | - | 9E-2 | |
| 29 | Sudden opening — MSSVs | NO OCC. | NO OCC. | - | 2E-2 | |
| 30 | Loss of Circulating water | 6E-2 | 2.4E-2 | 1.4E-2 | 5E-2 | 1.4E-1 |
| 31 | Loss of CCW | 3E-2 | 2.4E-2 | - | 2E-2 | 5E-2 |
| 32 | Loss of SRW | 3E-2 | 2.4E-2 | - | 5E-3 | |
| 33 | Turbine trip | 9E-1 | 3.9E-1 | 2.8E-1 | 1.2E+0 | 1.69E+0 |
| 34 | Generator Trip | 5.5E-1 | 2E-1 | 1.4E-1 | 4.6E-1 | 8.9E-1 |
| 35 | Loss of Station Power | 2.3E-1 | 1.2E-1 | 4.2E-2 | 1.5E-1 | 3.9E-1 |

| Cat | Transient Type | Reference Plant Design Data (CR-3862) | Limited Reference Plant data | Reference Plant Data (EPRI) | NUREG/ CR-3862 | Indigenous Data |
|---|---|---|---|---|---|---|
| 36 | Pressurizer Spray failure | 1.5E-2 | NO OCC. | 2.8E-2 | 3E-2 | |
| 37 | Loss of Power to plant systems | 1.1E-1 | 9.8E-2 | 3.4E-1 | 1.1E-1 | 2.7E-1 |
| 38 | trip — cause unknown | 4.5E-2 | 2.4E-2 | - | 8E-2 | |
| 39 | Auto trip — no transient | 1.2E+0 | 7.2E-1 | 5.6E-2 | 1.5E+0 | |
| 40 | Manual Trip — no transient | 2.7E-1 | 2.2E-1 | 8.5E-2 | 4.7E-1 | |
| 41 | Fire within Plant | 3E-2 | NO OCC. | - | 2E-2 | |

## TABLE A-VIII. HISTORY OF REACTOR TRIPS FOR US UNITS WITH DESIGNS SIMILAR TO THE REFERENCE PLANT

| Unit | Number of Reactor Trips Per Reactor Year (Power >80%) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | '84 | '85 | '86 | '87 | Avg. | '88 | '89 | '90 | '91 | '92 | Avg. |
| Palisades | 2 | 6 | 1 | 6 | 3.8 | 0 | 1 | ? | 3 | 5 | 2.3 |
| Maine Yankee | 6 | 5 | 6 | ESD | 5.7 | 2 | 2 | ? | 3 | 0 | 1.8 |
| Calvert Cliffs — 1 | 1 | 1 | 3 | 5 | 2.5 | 2 | 3 | ? | 1 | 0 | 1.5 |
| Millstone-2 | 2 | 1 | 2 | 5 | 2.5 | 1 | 1 | ? | 3 | 0 | 1.3 |
| St. Lucie-1 | 4 | 1 | 2 | 2 | 2.3 | 2 | 1 | ? | 2 | 1 | 1.5 |
| Calvert Cliffs — 2 | 0 | 0 | 3 | 5 | 2.0 | 2 | ESD | ? | 0 | 5 | 1.8 |
| Arkansas-2 | 9 | 9 | 3 | 2 | 5.8 | 2 | 2 | ? | 0 | 2 | 1.5 |
| St. Lucie-2 | 5 | 5 | 4 | 3 | 4.3 | 0 | 2 | ? | 0 | 2 | 1.0 |
| San Onofre-2 | 6 | 6 | 5 | 2 | 4.8 | 2 | 0 | ? | 1 | 1 | 1.0 |
| San Onofre-3 | 5 | 4 | 2 | 2 | 3.3 | 1 | 2 | ? | 1 | 1 | 1.3 |
| Waterford-3 | NCO | 5 | 6 | 5 | 5.3 | 2 | 3 | ? | 3 | 0 | 2.0 |
| Palo Verde-1 | NCO | NCO | 8 | 2 | 5.0 | 3 | 1eq | ? | 2 | 2 | 1.8 |
| Palo Verde-2 | NCO | NCO | 1 | 3 | 2.0 | ESD | 2eq | ? | 2 | 1 | 2.0 |
| Palo Verde-3 | NCO | NCO | NCO | NCO | n/a | 1 | 0eq | ? | 2 | 1 | 1.2 |

Most US utilities initiated formal Reactor SCRAM Reduction programmes in the mid-1980s.

The effectiveness of these programmes can be judged by the 57% reduction in annual trip frequency which has been achieved over the last 5 years:

- Average trip frequency, 1984 thru 1988 = 3.5 per unit year,
- Average trip frequency, 1988 thru 1992 = 1.5 per unit year,

### 1.10.3. Trends in reactor trip frequency — conclusions and insights

Review of the findings from Tables A-VII and A-VIII introduce some interesting insights because it appears that the greatest influence on trip frequency in US nuclear plants may have been the implementation of trip reduction programmes, rather than advances in plant design. There is only a marginal difference between the data for the older plants and those which have gone into service in the late 1970s to mid 1980s.

There was however, a dramatic change in plant trip frequency for all similar plants similar to the reference plant, during the late 1980s.

These facts complicate the prediction of trip frequency for the ALWR, because the actual experience could be dominated by the particular attention that plant managers pay to trip reduction, a condition which is very difficult to model. Trip reduction has tended to focus on the prevention of human errors of commission which have been a major contributor to avoidable reactor trips.

If the mature performance of ALWR is comparable to US plants, a prediction or goal for a trip frequency of about 1.5 per year would seem reasonable. This is the number that probably should be compared with the analytical results from the reliability models. Recommendations for changes to the design of ALWR should be deferred until differences between this 1.5 per year benchmark and the analytical predictions from the project have been fully rationalized and the reasons for any differences are well understood.

However, the analytical results should be evaluated to identify those important components where maintenance or test practices do have the potential for initiating a trip. This evaluation should then be followed with an assessment of the maintainability of these components to determine whether there are defensive measures which can be put in place before the plant goes into service. This in part will included in the component RCM evaluation.

### 1.10.4. Generic component failure rate database

A component level availability database was developed from ten separate sources to provide the necessary failure rate information needed for this project. The sources used to develop this database were:

- Generic Component Failure Data Base For Light Water and Liquid Sodium Reactor PRAs, February 1990, EGG-SSRE-8875
- EPRI, Reliability database for ALWR PRAs,
- IEEE Standard 500 (generally a secondary reference),
- NUCLARR,

- RELIABILITY DATA BASE, IAEA Compilation of Generic Component Reliability Data (DRAFT, 1988),
- EPRI AP-2071, Component Failure and Repair Data For Coal Fired Power Units, October 1981,
- No data available — estimated by comparison with similar components in the database or based on experience,
- GADS (1976–1985),
- Full-scale plant Safety and Availability Assessment — A Demonstration of GO system Analysis Methodology, July 1985, EPRI NP-4128,
- What every Engineer Should Know About Reliability and Risk Analysis, M. Modarres, 1993.

### 1.10.5. Limitations and assumptions in the component specific database

- Error factors (EF) and repair times were rounded off to the next highest whole number. If no information on data dispersion was available, an error factor of 10 was assumed,

- With few exceptions the database only included operating failure rates. If demand failure rates were needed, they were either taken from the standard PSA database or derived from the operating failure rates.

  To derive demand failure rates from operating failure rates it is necessary to make two assumptions:

  (i) That "standby failure rates" are the same as the "operating failure rates" (generally a conservative assumption in a moderate temperature, non-corrosive and clean environment),
  (ii) That "failure on demand" is due entirely to undetected failures which occur during standby operation.

  If these assumptions are valid, then the demand failure probability, “Lambda D”, can be found from the equation:

  "Lambda D" = "Lambda O" * T/2

  Where “Lambda O” is the operating failure rate and T is the average duration between functional operability tests of the component.

- A great deal of care had to be exercised in the application of the component repair time data, "Tau", provided in the database.

  The numbers provided are "typical average" values for all failure modes.

  In a plant specific application they may differ dramatically from the average. Repair data exhibits a great deal of plant to plant variation because the actual repair time depends upon component location, how accessible it is, whether special equipment is needed for the repair, whether needed rigging points are available, etc.

  Judgement was used to define appropriate plant specific repair times for important components, or to confirm the applicability of the generic data, before the results of the analysis were used to justify recommendations to improve component maintainability.

## 1.11. RESULTS

The operating experience data both for plants which are similar to the reference plant and for indigenous PWRs were combined with the analytical results from the unavailability and unreliability fault trees to provide a prediction of the expected magnitude of the unavailability from Forced outages, forced reductions and maintenance and refueling outages. The final results from this analytical activity are presented below.

### 1.11.1. Unreliability analysis and the prediction of FO or SCRAM rate

The results from the ALWR unreliability analysis, which represent a combination of historical data and analytical assessments, indicate that the ALWR can expect to experience a full forced outage due to SCRAM or immediate plant shutdown about 4 times per year. Provided that the ALWR design is similar to other current generation plants with similar design characteristics, this estimate should represent a reasonable prediction for mature plant operation. There is no evidence to suggest that this is not the case, and the operability and reliability is expected to be similar, although the analysis did not evaluate the possible effects on plant reliability if critical components are purchased from indigenous vendors.

Two important influences on FO/SCRAM rate were not explicitly credited in this analysis:

– The ability of the operator to detect impending failures and intervene to prevent a SCRAM or shutdown either by:
  (i) Reducing power to allow degraded equipment to be removed from service before it fails, or,
  (ii) Realigning standby equipment to effect a "bumpless" transfer between operating and standby equipment when the operating equipment shows evidence of degradation,
– Errors of commission in which operator and maintainer errors initiate SCRAM.

> This issue was important to US plants prior to the implementation of rigorous trip reduction programmes in the mid-1980s, but is currently less important. The contribution has been implicitly included with the provision of a historical contribution for "maintenance errors" in the final analysis

These issues were not explicitly modeled in the fault trees because treating them with fidelity is very difficult, and in the case of errors of commission, fraught with high levels of uncertainty. However, the influences from these two factors are very real and their inclusion must be considered if the analytical results are to serve as a predictive tool which can demonstrate that the ALWR will be expected to meet its assigned availability goals.

To account for the positive influences that the plant operators can have on trip frequency, the analytical results were modified to include high level historical data which already contains the effects of these influences. The cutset results from the reliability model were used to augment the historical data, where it was used, by providing an intimation of the many potential causes for failure which could also be used to direct decision making and provide needed insights which could form the basis for recommendations for change.

A summary of the rank ordered contributors to full FO and their individual contributions are shown in Table A-X.

### 1.11.2. Unavailability analysis

*1.11.2.1. Unavailability due to full forced outage*

As described earlier, the final analysis used to predict the forced outage rates and unavailabilities for the ALWR represents a combination of historical and analytical data. The individual sources used to predict the impact of each identified contributor is shown in Table A-XI.

TABLE A-IX. RANKED LIST OF UNAVAILABILITY CONTRIBUTORS CANDIDATE SYSTEMS/EQUIPMENT FOR RCM

| Contributors to Forced Outages | Annual hours lost generation |
|---|---|
| Steam Generator | 107–162 |
| Feedwater | 22–62 |
| Loss of RCS Flow & PZR SVs | 32–69 |
| Main Turbine, MS/R | 31–104 |
| Dropped CEA, RRS | 11–17 |
| RPS (spurious) | 1–15 |
| Generator & Main Xfmr | 13–26 |
| Offsite Power | 11 |
| Main Steam, MSSVs, ATBVs, MSIVs | 7–8 |
| Extraction Steam | 7 |
| CVCS & L/D HX | 6 |
| Circulating Water | 5 |
| CCW, ESW, EChW | 1–4 |
| I&C Power | 3 |
| Switchyard, Aux XFmr, 13.8 KV | 1–3 |
| DC Power | 3 |
| Condensate & condenser tubes | 2 |
| Instrument Air | 1 |
| TBCCW/TBOCCWS | 1 |
| Fire Protection | 1 |
| S/G Blowdown | 1 |
| Following Items Included but not ranked because not amenable to RCM | |
| Maintenance errors | 6 |
| Manual S/D | 14 |
| 480vac LC | 1 |
| **Total** | **381** |

## TABLE A-X. SUMMARY OF RESULTS — AVAILABILITY ANALYSIS

| Contributor to plant Unavailability | Annual Frequency | Annual full power hours of lost generation | Total Unavailability Contribution |
|---|---|---|---|
| Full forced outages | 3.90 | 391 | 4.46 |
| Forced Reductions | N/A | 43 | 0.50 |
| Maintenance Outages | 0.45 | 130 | 1.48 |
| Scheduled Refueling outages | 0.67 | 1206 | 13.77 |
| Total | | | 20.21 |

## TABLE A-XI. SUMMARY OF RESULTS — RELIABILITY ANALYSIS

| Cause of SCRAM or immediate shutdown | Source of Frequency Estimate | Annual contribution to FO/SCRAM frequency |
|---|---|---|
| Turbine trip | Historical | 0.80 |
| Steam generator tube leak/rupture | Analytical | 0.53 |
| Loss of RCS flow | Historical | 0.46 |
| Loss of feedwater | Analytical | 0.43 |
| Premature operation of MSSV | Analytical | 0.25 |
| Maintenance errors | Historical | 0.25 |
| Dropped CEA | Analytical | 0.17 |
| MS/R | Historical | 0.14 |
| Main generator trip | Historical | 0.18 |
| Manual S/D — LCOs | Historical | 0.11 |
| Letdown HX | Analytical | 0.09 |
| Condenser tubes | Historical | 0.07 |
| CVCS induced | Analytical | 0.07 |
| Atmospheric TBVs | Analytical | 0.05 |
| High RCS pressure | Analytical | 0.05 |
| Low RCS pressure | Analytical | 0.05 |
| Pressurizer SVs | Analytical | 0.04 |
| TBCCW/TBOCW | Analytical | 0.03 |
| Loss of 13.8 KV bus | Analytical | 0.03 |
| Loss of 480vac load center | Analytical | 0.02 |
| Spurious Rx SCRAM (RPS) | Analytical | 0.02 |
| High power (RRS) | Analytical | 0.01 |
| Main Xfmr — fault | Analytical | 0.01 |
| Aux. Xfmr — fault | Analytical | 0.01 |
| Closure of MSIVs | Analytical | 0.01 |
| Loss of ESW | Analytical | 0.01 |
| Essential chilled water | Analytical | 0.01 |
| | Total | 3.90 |
| General I&C<br>- not an independent contributor | Historical | 0.93 |
| | Total (incl. general I&C) | 4.83 |

**Predicted unavailability = 391 h/a = 0.0446 = 4.5%**
**due to forced outages**

If the **"general I&C"** category is **included,** this predicted unavailability **increases to 4.9%.**

When the effects of regulatory shutdowns are excluded from US data, the calculated unavailability of 4.5% compares favorably with the 7.5% historical US nuclear plant unavailability due to full forced outages (Table A-XI). This difference may reflects the potentially improved operability and reliability characteristics of the design for the ALWR when compared to earlier plants of similar design. These differences result from:

- The use of a digital feedwater control system,
- Installation of a deaerator in the feedwater system to provide some surge capacity,
- Increased redundancy in the condensate and feedwater trains and the absence of a pumped forward heater drain system,
- A reactor power cutback system and 100% turbine bypass capability.

Exclusion of unavailability contributions from regulatory and safety issues in this comparison is justified by a perception that there are significant differences between the USA and the indigenous regulatory environments and that the expected impact on plant unavailability from regulatory actions and licensing issues will be much lower.

*1.11.2.2. Prediction of unavailability contributions from forced reductions (equivalent unavailability)*

The analytical predictions of the equivalent availability for ALWR represent an annual generation loss due to forced reductions which is equivalent to 43 full power hours per year or about 0.5%.

The primary contributors to this originate within the condensate and feedwater system and reflect the need to reduce power to deal with:

- Condenser tube leaks and dirty condenser tubes,
- High pressure feedwater heater leaks,
- Miscellaneous problems within the feedwater and condensate system:
  - Strainer, valve and pump failures,
- Miscellaneous problems within the circulating water system:
  - Strainers and valves.

*1.11.2.3. Prediction of unavailability contributions from planned and scheduled outages*

The data provided in the tables provided in Tables A-IV through A-X was analyzed to provide fractional estimates of the expected maintenance and refueling outage lengths and to calculate the average refueling outage lengths which can be expected for a nuclear plant with a similar reference design. The results of this analysis are presented in Table A-XIII and used to calculate the expected frequency for maintenance outages, their expected lengths and the expected durations for refueling outages.

The results of the analysis led to the following assessments for plants similar to the reference design.

TABLE A-XII. SUMMARY OF RESULTS — UNAVAILABILITY DUE TO FULL FORCED OUTAGES

| Cause of SCRAM or immediate Shutdown | Annual FO/SCRAM Frequency | MDT** (h) | Unavailable h/a |
|---|---|---|---|
| Turbine trip | 0.80 | 125 | 100 |
| Steam generator tube leak/rupture | 0.53 | 202 | 107 |
| Loss of RCS flow | 0.46 | 140 | 64 |
| Loss of feedwater | 0.43 | 51 | 22 |
| Premature operation of MSSV | 0.25 | 24 | 6 |
| Maintenance errors | 0.25 | 24 | 6 |
| Dropped CEA | 0.17 | 106 | 18 |
| MS/R | 0.14 | 29 | 4 |
| Main generator trip | 0.18 | 139 | 25 |
| Manual S/D — LCOs* | 0.11 | 126 | 14 |
| Letdown HX | 0.09 | 24 | 2 |
| Condenser tubes | 0.07 | 24 | 2 |
| CVCS induced | 0.07 | 24 | 2 |
| Atmospheric TBVs | 0.05 | 24 | 1 |
| High RCS pressure | 0.05 | 24 | 1 |
| Low RCS pressure | 0.05 | 24 | 1 |
| Pressurizer SVs | 0.04 | 125 | 5 |
| TBCCW/TBOCW | 0.03 | 30 | 1 |
| Loss of 13.8 KV bus | 0.03 | 57 | 2 |
| Loss of 480 v load center | 0.02 | 57 | 1 |
| Spurious Rx SCRAM (RPS) | 0.02 | 24 | 1 |
| High power (RRS) | 0.01 | 24 | 1 |
| Main Xfmr — fault | 0.01 | 143 | 1 |
| Aux. Xfmr — fault | 0.01 | 100 | 1 |
| Closure of MSIVs | 0.01 | 24 | 1 |
| Loss of ESW | 0.01 | 30 | 1 |
| Essential chilled water | 0.01 | 30 | 1 |
|  | 3.90 |  | 391 |
| General I&C<br>- not an independent contributor | 0.93 | 41 | 38 |
|  | 4.83 |  | 429 |

[*] The difference in regulatory climate between the IAEA member state building the ALWR and the USA was assumed to result in an indigenous average shutdown time for regulatory and safety problems being 1/10th of the average plant down time experienced in the USA (assumption without basis — no comparable data available)

[**] MDT data calculated as a weighted average from historical data, the plant specific database, or assigned a minimum value of 24 hours. 24 hours was assumed to be the average minimum time required to return to power following a plant trip.

TABLE A-XIII. COMPARISON BETWEEN THE OPERATING EXPERIENCE FOR ALL INDIGENOUS REACTORS, 1980–1991, AND THE PREDICTIONS FOR ALWR

| Contributors to Forced Outages | PWR Operating Data | | | Prediction for ALWR | | | |
|---|---|---|---|---|---|---|---|
| | FO Freq. | FO Duration | h/a | | FO Freq. | FO duration | h/a |
| Steam Generator | 0.40 | 338 | 162 | Steam Generator | 0.53 | 202 | 107 |
| Feedwater | 0.87 | 71 | 62 | LOFW | 0.43 | 51 | 22 |
| RCS | 0.22 | 146 | 32 | LO RCS Flow<br>PZR Svs | 0.46<br>0.04 | 140<br>125 | 64<br>5 |
| Main Turbine | 0.63 | 49 | 31 | Turbine Trip<br>MS/R | 0.80<br>0.14 | 125<br>29 | 100<br>4 |
| CEDM | 0.39 | 45 | 17 | Dropped CEA<br>Hi Pwr (RRS) | 0.17<br>0.01 | 106<br>24 | 18<br>1 |
| RPS | 0.26 | 58 | 15 | Spurious | 0.02 | 24 | 1 |
| Main Power (incl.gen) | 0.29 | 46 | 13 | Generator trip<br>Main Xfmr | 0.18<br>0.01 | 139<br>143 | 25<br>1 |
| Offsite Power | 0.29 | 36 | 11 | | | | |
| Main Steam | 0.43 | 17 | 7 | Prem. Op. MSSV<br>Atmos. TBVs<br>Closure MSIVs | 0.25<br>0.05<br>0.01 | 24<br>24<br>24 | 6<br>1<br>1 |
| Extraction Steam | 0.05 | 136 | 7 | | | | — |
| Circulating Water | 0.14 | 32 | 5 | | | | - |
| CCW | 0.05 | 91 | 4 | ESW<br>Ess. Ch.Water. | 0.01<br>0.01 | 30<br>30 | 1<br>1 |
| I&C Power | 0.17 | 19 | 3 | | | | - |
| Switchyard | 0.10 | 33 | 3 | Aux XFMR<br>13.8 Kv bus | 0.01<br>0.03 | 100<br>57 | 1<br>2 |
| DC Power | 0.10 | 27 | 3 | | | | - |
| Condensate | 0.10 | 24 | 2 | Condenser tubes | 0.07 | 24 | 2 |
| Instrument Air | 0.05 | 22 | 1 | | | | - |

| Contributors to Forced Outages | PWR Operating Data | | | Prediction for ALWR | | | |
|---|---|---|---|---|---|---|---|
| | FO Freq. | FO Duration | h/a | | FO Freq. | FO duration | h/a |
| TBOCCWS | 0.02 | 23 | 1 | TBCCW/ TBOCCW | 0.03 | 30 | 1 |
| Fire Protection | 0.02 | 15 | 1 | | | | - |
| S/G Blowdown | 0.02 | 11 | 1 | | | | |
| | | | | CVCS<br>Hi RCS press<br>Lo RCS press<br>Letdown HX | 0.07<br>0.05<br>0.05<br>0.09 | 24<br>24<br>24<br>24 | 2<br>1<br>1<br>2 |
| | | | | Maint. Errors | 0.25 | 24 | 6 |
| | | | | Manual S/D | 0.11 | 126 | 14 |
| | | | | 480vac LC | 0.02 | 57 | 1 |
| Total | 4.60 | | 381 | | 3.90 | | 391 |

*1.11.2.4. Unavailability from (planned) maintenance outages*

Using the technique of weighted averaging to find the "expected" maintenance outage duration, the expected maintenance outage duration is 289 hours. However, the frequency for these maintenance outages appears to be about 0.45 (one every other year) so the expected loss per year is 130 hours. The rationale for this assessment is provided below:

Maintenance outage frequency = 47/105 = 0.45/a
Average duration for maintenance outage = 289 h
so,
Expected maintenance outage hours = 289 * 0.45 = 130 h/a

This represents an unavailability contribution of 1.48%.

Unavailability from (scheduled) refueling outages:

– The average length for "normal" refuelings for the entire database is 1905 hours,
– Limiting the evaluation to the "normal" refueling outages for 1991–1992 indicates an average refueling length of 1749,

- When data is limited to inclusion only of the 1991–1992 experience with the "normal" refuelings for the three plants closest in design to the ALWR, an average refueling outage of 1952 hours is indicated,
- The history for indigenous plants of all types indicates an average refueling outage length of 1807 hours.

### 1.11.3. Conclusions

Though an analysis of the refueling outage data for US PWRs of similar design shows that an average refueling takes about 1900 hours, in recent years this average has seen marked decrease until it has reached approximately 1750 hours. This is in large measure due to better planning and scheduling of maintenance activities and a reduction in the number of plant modifications.

Editor's Note:
Recent achievements have indicated that the declining trend outage lengths is continuing and anecdotal evidence from 1996, suggests that US utilities are now frequently achieving outage lengths of approximately 40 days (960 hours).

The historical data for indigenous PWRs for the past 15 years shows an average refueling outage of 1807 hours. Since the average duration for an indigenous PWR refueling outage falls between the recent and long-term US plant averages. it is reasonable to predict, with a high degree of confidence, that the expected refueling outage duration for ALWR will follow current trends and that the goal of 1800 hours per refueling will be easily achieved.

Because the ALWR will operate on an 18 month fuel cycle, the hours lost each refueling outage hours will be accrued over more than a full operating year. To calculate the average annual contribution to unavailability, the probability of a refueling outage occurring in any given year is assumed to be 0.67. This means that the average annual hours of lost generation due to refueling outages will be 1206.

### 1.11.4. Summary of results

A summary of the analytical results from the RAM analyses and the actuarial information used to augment this analytical information to provide predictions of the expected reliability, availability and maintainability levels for the ALWR, are presented in tabular form by:

- Table A-IX: Ranked List of Unavailability, Contributors Candidate Systems/Equipment for RCM,
- Table A-X: Summary of Results — Availability Analysis,
- Table A-XI: Summary of Results — Reliability Analysis,
- Table A-XII: Summary of Results — Unavailability due to Full Forced Outages,
- Table A-XIII: Comparison Between the Operating Experience for All Indigenous Reactors, 1980–1991, and of the Predictions for ALWR,
- Table A-XIV: Distribution of Maintenance and Refueling Outage Lengths for US plants of similar design, 1981 through 1992.

TABLE A-XIV. DISTRIBUTION OF MAINTENANCE AND REFUELING OUTAGE LENGTHS FOR REFERENCE-TYPE PLANTS, 1981 THROUGH 1992

| Fraction of outages | Maintenance outage duration | Fraction of outages | Refueling outage duration |
|---|---|---|---|
| 20/47 | 0–200 h | 5/41 (12.2%) | 600–1000 h |
| 9/47 | 200–400 h | 5/41 (12.2%) | 1000–1500 h |
| 8/47 | 400–600 h | 17/41 (41.5%) | 1500–2000 h |
| 5/47 | 600–800 h | 8/41 (19.5%) | 2000–2500 h |
| 3/47 | 800–1000 h | 2/41 (4.9%) | 2500–3000 h |
| 2/47 | >1000 h | 2/41 (4.9%) | 3000–3500 h |
| | | 1/41 (2.4%) | 3500–4000 h |
| | | | 4000–5000 h |
| | | 1/41 (2.4%) | > 5000 h |
| | | Average Length (normal refuelings–U.S) | 1905 |
| | | Average Length (91–92–USA) | 1749 |
| | | 3 US Plants Similar to Reference plant | 1952 |
| | | Indigenous PWRs | 1807 |

## 1.12. INSIGHTS AND RECOMMENDATIONS

The results from the RAM analysis identified nothing specific which could lead to a conclusion that there are any obvious plant design deficiencies which will have a negative impact on the life-cycle economy of the ALWR. In fact, when compared to earlier plants, the increased redundancy in the feedwater system, the power cutback system, 100% turbine bypass capacity and an ability to use fast valving on the turbine generator to reduce power and support hotel loads without a reactor SCRAM, are all positive influences, and eventually are expected to show that the ALWR is capable of operating with a very low SCRAM rate.

However, the insights provided by the results from the analysis were used to develop a set of recommendations which were expected to have an important influence on the future performance of the plant. Because the plant protective and control systems listed above must operate reliably if they are to achieve their full potential in minimizing SCRAM rates and maintain power plant operability under transient conditions, they must have high availabilities and reliabilities. This means that their maintenance and testing programmes must be effective and should be formally included in any plant initiatives associated with the implementation of RCM or optimized test and maintenance programmes. This leads to Recommendation Nr 1.

**Recommendation No. 1: Test and maintenance programme for MFW control and the reactor power cutback system**

Because these systems interface functionally with trip sensitive components, and they must be maintained at power, there must be a well thought out and well constructed programme for test and maintenance which ensures that:

- The availability and reliability of these systems is optimized,
- Procedures used to guide the maintenance of the important systems are constructed in a way which will minimize the likelihood human errors occurrence to induce system failure and a consequential SCRAM.

**Recommendation No. 2: Prevent spurious feedwater system failures (I&C)**

Historically, nuclear plant feedwater control systems have experienced a number of unexplained trips, often during the performance of routine on-line I&C maintenance, test and troubleshooting activities. In many cases these unexpected events could perhaps be traced to the problems which are sometimes encountered with systems which are designed to have an isolated ground loop. If an isolated ground system experiences an initial ground fault there is no observable effect on system operation. However, if second ground fault is accidentally initiated during maintenance (insertion of test instrumentation probes), the ground-fault loop provides a sneak path for electrical current and can result in inadvertent actuation/de-energization of system components and, occasionally, a plant trip,

To avoid this problem, it is necessary to install a ground detection system for DC and Instrument AC systems which have isolated grounds and implement procedures to monitor them. Since the detection system does not generally indicate where the ground is located, the control room staff must monitor it continuously. When a ground is detected, they must immediately identify all ongoing maintenance and test activities, and from this infer where the ground may have introduced. In this way, unwanted grounds can be detected, located and corrected quickly, before a second ground fault can be introduced and lead to unexpected system behavior.

**Specific recommendation:** Confirm that a DC ground detection system is in place for all isolated ground loops which have the potential to initiate plant SCRAM, and initiate operational procedures to monitor, detect and correct grounds whenever they occur.

**Recommendation No. 3: Optimize turbine generator reliability**

The main turbine-generator set is expected to be one of, if not the, most important contributor to the ALWR SCRAM rate. There is little or no flexibility in the selected turbine generator design so to identify and suggest design modifications is probably neither feasible nor productive. However, a great deal can be done with a comprehensive design review and an effective test and maintenance programme which ensures that the turbine generator and all of its protective and support systems operate with maximum reliability and availability. This will provide two benefits:

- It will minimize the rate turbine-generator trips which are initiated by failed components,
- It will minimize the amount of on-line maintenance, each event of which represents an opportunity for a trip induced by human error.

For the ALWR, a programme of this type can have many facets, each of which is exemplified by the following recommendations and should be considered as candidates for implementation.

**Recommendation No. 4: Implement a turbine-generator test and maintenance programme**

Review all extant turbine vendor information bulletins, field modification notices and similar documents and confirm that all past vendor requirements or recommendations for modification or change are implemented in the equipment provided for the ALWR, prior to start-up.

- Confirm that the test and maintenance programme for the ALWR encompasses all vendor requirements and recommendations, by function and periodicity, and that all other important components are brought under the aegis of an RCM programme. Of particular concern may be the maintenance and operability of all monitoring and diagnostic equipment which can be used to detect impending problems and allow the operator to intervene before failure occurs,
- Consider the implementation of special external marking (red tag, label or paint) on all components which can initiate a T-G trip. This is to alert maintainers to the risks of maintaining these components on-line. Typical of the components which have historically contributed to spurious T-G trips during maintenance are:
  (a) Feedwater heater level switches,
  (b) MS/R high level switches,
  (c) Control and instrument power panels,
  (d) Local turbine generator trip sensors, actuators and their power supplies.

**Recommendation No. 5: Minimize the number of reactor coolant pump failures and prevent loss of RCS flow trip**

The RCPs have historically been an important contributor to plant SCRAM rate because if there is an RCP trip, there are few, if any, options available to the operator which can be implemented to prevent SCRAM. The reliability analysis for this system showed that failure of protective and control instrumentation, loss of lubrication caused by low oil reservoir level and RCP seal failures are important contributors to pump unreliability. These issues can be addressed in several ways.

- **Implementing effective test, monitoring and diagnostic programme for RCPs**

  Confirm including the RCPs and all of their auxiliary support systems into the ALWR RCM programme and that this programme encompasses all vendor requirements and recommendations by function and periodicity. Of particular concern may be the maintenance and operability of all monitoring and diagnostic equipment which can be used to detect impending problems and allow the operator to intervene before serious or catastrophic failure occurs.

  If not already part of the design, consider the installation of on-line vibration monitoring and spectrum analysis equipment to provide diagnostic monitoring functions. Most mechanical failures will be evidenced and diagnosed by a shift in the vibration spectrum long before they become catastrophic. Vibration amplitude measurement alone, will not provide this capability.

**Recommendation No. 6: Minimize the frequency for RCP seal failures**

Maximize the inherent RCP seal life by confirming that the design and recommendations for operating the RCPs in the ALWR reflect the latest research performed by EPRI, the Owner's Group and pump vendors.

**Recommendation No. 7: Prevent RCP motor failure caused by RCP L.O. reservoir level**

Confirm that normal operating surveillance procedures include monitoring the L.O. reservoir level and ensure that whenever the make-up rate reaches a predetermine threshold, there is an investigation into cause and initiation of any effective maintenance strategies at the first available opportunity. A single, short period of operation at very low L.O. reservoir level may cause irreversible damage to the RCP motor bearings.

**Recommendation No. 8: Minimize the frequency for steam generator tube leakage/rupture events**

After an initial period of operation in which there may, or may not be infant mortality, the failure rates for mechanisms which lead to steam generator tube leaks or rupture tend to increase, i.e. they are time dependent. This increase in failure rate, sometimes considered to be "ageing" must be minimized so that the eventual time to failure for individual tubes is maximized. This means that:

- Vendor recommendations for inspection and maintenance of steam generators must be followed and that secondary side chemistry requirements must be clearly and unambiguously identified in the relevant operating procedures,
- **Steam generator chemistry must be strictly controlled**;
  This leads to a requirement that the condensers are well maintained to prevent ingress of chloride salts, and that the condensate demineralizers and the condensate and feedwater monitoring system is maintained at its optimum level of performance.

  This can be achieved by confirming that in-plant programmes meet the above requirements and that there is an effective test and maintenance programme in place for the condensate and feedwater monitoring system

**Recommendation No. 9: Implement an active SCRAM reduction during plant operation**

The US data (Table A-XI) shows that a significant reduction in trip rates began in the mid-1980s and was sustained into the 1990s. This was, in large measure, due to the implementation of formal trip reduction programmes at all US nuclear plants. Indigenous plants can capitalize on this experience by following suit if they have already done so, although the current history indicates that there may be opportunities for improvement in this area.

A comprehensive SCRAM reduction programme contains several major elements which have the same objective, "prevention of the reoccurrence of known trip initiating events or conditions". Examples of some of the general types of activities which can have the effect of reducing SCRAM frequency are described below.

– **Learn from past experience** by reviewing the historical trip data and identifying their potential causes — initially, this approach will be of limited application to the ALWR because it has no operating experience. Comparison of the similarities between the conditions expected at the EALWR with those present at the time of the failures in the other plants, and an assessment of whether they could or could not occur, may however be useful;

– **Find the cause for every SCRAM and prevent its reoccurrence**
The most important activity associated with SCRAM reduction is one of identifying its root causes — real root causes, not the symptoms. For example, "Random hardware failure from unknown causes" and "failure to follow procedures" are symptoms of underlying problems, not root causes.

Successful root cause analysis requires structure and training in the necessary skills and their programmematic application is finding the cause for every SCRAM. The goal of the root cause analysts should be "to never have the same SCRAM twice for the same reason". This carries with it the implication that root cause analysis must also be accompanied by a rigorous implementation programme for all changes which are recommended. The root cause analysis should also provide the reasons that existing plant programmes maintenance and test programmes did not prevent the failure from being detected and corrected.

– **Increase awareness amongst plant staff**
If staff are innately aware of the potential causes for SCRAM and are reinforced in recognizing the importance of not having SCRAMs, the SCRAM rate originating with errors of omission and commission will decrease. Typical activities include:
(a) Confirming that all plant components are clearly identified, have unambiguous and clearly understandable identifiers and that the identification tags indicate the normal operating state (e.g. red marker — valve normally open during operation, green marker — valve normally closed during operation),
(b) Using special markings to identify components or equipment which can initiate SCRAM (particularly instrumentation),
(c) Optimizing the amount of on-line maintenance,
(d) Making sure that all plant staff members are aware of the causes for past trips by publishing details of the event and any results which come from root cause analyses. This information should be provided in easily read, bulletin format.

Implementation of the general recommendations provided above should minimize the frequency of occurrence for more than 75% of the identified contributors to reactor SCRAM,

– **Recommendations to minimize unavailability contributions from forced reductions (equivalent unavailability)**

The relatively small contribution to lost generation which is represented by the predicted equivalent unavailability of 0.5% implies that there is little that can be meaningfully changed within the current hardware design. The ALWR already has sufficient redundancy in the circulating water, condensate and feedwater systems to ensure that the generation loss from forced reductions is likely to be about 30% of the losses experienced in earlier generations of plants. Historically, equivalent unavailability has ranged from 1.5% to 2.5% for these plants. Those outside this range have generally experienced unanticipated design deficiencies, often within the condensers.

The insights from the results of the equivalent availability analysis indicate that the recommendations which seem appropriate for the ALWR should focus on providing assurance that the installed hardware operates with its expected levels of reliability and availability and not on providing additional hardware to compensate for the few failures which may occur.

**Recommendation No. 10: Implement an RCM programme for important plant equipment**

The implementation of an RCM programme for balance of plant systems, turbine/generator and auxiliaries, circulating water, condensers, condensate, feedwater and associated control systems will have many benefits because it will:

- Assure that BOP components achieve their inherent levels of reliability so that the number of plant transients and load reductions are minimized;
- Maximize the availability of those components which are redundant during full power operation so that should an unexpected failure of a power producing component, the probability of a successful start and run is maximized for the back-up;
- Optimize the amount of on-line maintenance which is required. Many trips and sudden load rejections which NPPs have experienced in the past, resulted from the attempts of plant maintainers to troubleshoot, adjust and repair control systems while at power.

**Recommendation No. 11: Confirm that the installed monitoring and diagnostic equipment is adequate for critical components**

The reduction of transients and load reductions depends very heavily on the ability of the plant operating staff to understand the internal condition of critical hardware. This means that when degraded conditions occur, the staff can initiate a manual start of any available standby equipment and effect a "bumpless" transfer between operating and standby hardware. This minimizes the reliance on automatic transfer which must follow a catastrophic or sudden component failure and the likelihood that a plant upset condition is initiated.

This knowledge also allows the repair and refurbishment of hardware during any unplanned or planned outage so that the need for on-line maintenance is minimized.

The following approach can be used to review the adequacy of diagnostic and monitoring equipment for critical hardware:

- Identify all critical hardware components. These are typically those system components which provide an active function during normal power operation:
  (a) Pumps, drivers and auxiliary dependent systems,
  (b) Heat exchangers,
  (c) Control system components and control valves,
  (d) Protective hardware such as strainers, relief valves and component trip systems.

  The cutsets for the equivalent availability and reliability models will provide a basis for this list, although because of "modularization" and simplification within the model, some individually important components may not be explicitly identified.

- Identify each of the important functional failure modes for each of the critical components and confirm that the installed instrumentation will identify the effect of the failure mode so that condition can be inferred. A few typical examples might be:
  (a) Vibration monitors (and spectrum analyzers) for rotating equipment,
  (b) Leakage and delta P/delta T sensors for heat exchangers,
  (c) Flow and pressure monitors for leak-off, cooling and lubrication loops,
  (d) Temperature monitors downstream of drain valves, steam traps, relief valves etc. to allow the detection of leakage,
  (e) Alarmed level monitors for all equipment where water or condensate accumulation can initiate turbine trip
  (f) Ground detectors on systems which have an isolated ground loop.

  Confirm that the information is presented in a way which allows diagnosis of condition within the time available to intervene and prevent progression to a higher damage state (complete failure), i.e. confirm that important information can be detected and processed in a timely manner by the control room operators, or, if the information is provided locally, that it is collected and **analyzed** periodically by the ex-control room operators.

**Recommendation No. 12.: Perform a maintainability review for all critical components**

A maintainability review can best be made during construction because it is only at that time that there is a reasonable opportunity to change the plant at low cost. Typical of the items which should be part of the maintainability review for critical equipment includes confirmation that:

- Repair of the equipment for all important component failure modes can be of rigging and lifting points,
- Accomplished without removal of piping interferences, the removal of cable trays. or the installation Closed vessels which may require entry for repair can be purged and cooled quickly,
- There is adequate clearance around the equipment for laydown, there is complete access for removal of all important component sub-assemblies, and there is access for any specially required maintenance equipment,
- There is local access to needed maintenance support systems, i.e. plant air and water, welding and power outlets,
- There is easy access to instrumentation and I&C control loops which may require testing, checking, calibration or repair,
- The lighting, ventilation and radiation protection provided in the areas around critical components is adequate to support effective repair.

The results of the maintainability analysis and the implementation of any needed changes will assure improved availability of plant equipment by maximizing the efficiency of the repair process and minimizing the effective mean time to repair (MTTR) for all critical plant components. These kinds of recommendations can best be implemented while the plant is under construction.

**Recommendations to minimize unavailability contributions from maintenance and scheduled outages**

Because the contribution to total plant unavailability from refueling and maintenance outages is by far the largest of all, it also provides the greatest opportunity for unavailability reduction. To exploit the potential for improvement in this area, the following broad general suggestions are offered. These suggestions are intended to typify the activities which could be initiated, rather than represent an exhaustive list of specific actions to implement:

**Recommendation No. 13: Consider implementation of each of the following activities as an integral part of a maintainability review for all critical components and equipment installed in the ALWR**

Attempt to minimize the overall amount of maintenance which must be performed during the refueling outage by:

- Identifying each major piece of equipment which is normally subject to overhaul or refurbishment during refueling,
- Perform an RCM study for each of these pieces of equipment and identifying the minimum set of tasks which whose performance assures effective maintenance,
- Confirm that the periodicity of the maintenance tasks is optimum each refueling.

Minimize the time required to perform maintenance on each major piece of equipment identified for the RCM programme by performing a maintainability analysis which ensures that:

- Access to the equipment is optimal, e.g. confirm that seismic restraints do not prevent adequate access for men and equipment or lack of shielding does not restrict access to the work site and that there is adequate laydown area for parts and maintenance equipment,
- Equipment layout does not result in severe interferences, e.g. piping and cable trays do not hinder disassembly,
- All required rigging points and equipment are installed if component must be rigged out of place for maintenance, disassembly or replacement.

Minimize the number of required high impact surveillance tests by implementing a programme which capitalizes on the availability of a PRA and the ability to request "cost beneficial licensing actions (CBLA)", e.g. minimize the frequency for structural integrity and integrated and local leak rate testing for the containment.

- Utilize the PRA to better define the plant "Q" list so that the number of components whose maintenance must be considered "safety related" is held to a minimum. This can save time and resources normally spent in maintaining components during an outage,
- Review the testability of the instrument and control loops within containment to ensure that they can be accessed easily for the required annual/refueling interval calibrations.

**Final recommendation: Use the candidate list of systems for RCM to guide programme implementation**

The results of the availability analysis were reviewed to identify those systems whose unreliability and attendant unavailability made them candidates for an RCM programme. This list is predicated upon the assumption that implementation of an RCM programme will enhance system reliability and improve overall plant performance. Implementation of RCM can also be used to reduce the overall maintenance by limiting the activities to those which are known to be effective.

Because the data needed to support selection of a system as a candidate for RCM on the basis of reduced maintenance is not part of the availability analysis, this second criteria must be applied separately and used to reorder or augment the items on the list shown in Table A-IX.

## 2. CASE STUDY # 2: RISK BASED PRIORITIZATION OF MOTOR OPERATED VALVES AT THE WASHINGTON NUCLEAR PLANT 2

(Refer to original paper written by L.T. Pong and R.N.M Hunt, and presented at the ANS International Topical Meeting, Seattle, September 1995)

This case study exemplifies the use of PSA to prioritize SSCs and demonstrates how probabilistic information from the PSA must be blended together with deterministic engineering insights to produce the required results. In this particular case, the focus was on the prioritization of motor operated valves (MOVs), however, an similar process would have been used to proritize any other class of SSC within the plant.

## 3. CASE STUDY #3: COMMON CAUSE FAILURE ANALYSIS OF MOTOR OPERATED VALVES AT THE WASHINGTON NUCLEAR PLANT 2

(Refer to original paper written by L.T.Pong and R.N.M Hunt, and presented at the ANS International Topical Meeting, Seattle, September 1995

This case study is introduced for a very important reason.

In the ALWR, an increase in the reliability of the success paths for each critical function can be expected as designers exploit their ability to combine redundancy and diversity of active systems with the high inherent levels of reliability provided by passive systems. The effects of these cahanges will appear with the predominanance of common cause failures (CCFs) as the primary contributors to functional unreliability. This case study provides some insights into the ways that the O-RAP programme will have to seek, find and defend against common cause failures.

# BIBLIOGRAPHY

The following bibliography provides a selected listing of reports, papers and journal articles which can be used as the starting point for any specific RAM or PSA activity which may be associated with the implementation of D-RAP or O-RAP. This listing of sources is by no means exhaustive, but should allow the user to identify other sources.

## 1. IAEA publications

- Manual on Maintenance of Systems and Components Important to Safety (Technical Reports Series, No. 268), 1986.
- Methodology for the Management of Aging of Nuclear Power Plant Components Important to Safety (Technical Reports Series, No. 338), 1992.
- Data Collection and Record Keeping for the Management of Nuclear Power Plant Aging: A Safety Practice (Safety Series No. 50-P-3), 1991.
- Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1): A Safety Practice" (Safety Series No. 50-P-4), 1992.
- Treatment of External Hazards in Probabilistic Safety Assessments for Nuclear Power Plants: A Safety Practice (Safety Series No. 50-P-7), 1995.
- Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2): Accident Progression, Containment Analysis and Estimation of Accident Source Terms: A Safety Practice (Safety Series No. 50-P-8), 1995.
- Evaluation of Fire Hazard Analyses for Nuclear Power Plants: A Safety Practice (Safety Series No. 50-P-9), 1995.
- Human Reliability Analysis in Probabilistic Risk Assessments for Nuclear Power Plants: A Safety Practice (Safety Series No. 50-P-10), 1995.
- The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteriain Nuclear Power Plant Safety: A Safety Report (IAEA Safety Series No. 106), 1992.
- Probabilistic Safety Assessment: A Safety Report (Safety Series No. 75-INSAG-6), 1992.
- Basic Safety Principles for Nuclear Power Plants (Safety Series No. 75 -INSAG-3), 1988.
- Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installations (Safety Series No. 50-C/SG.Q), 1996.
- Development of Safety Principles for the Design of Future Nuclear Power Plants (IAEA-TECDOC-801), 1995.
- Terms for describing new, advanced nuclear Power Plants (IAEA-TECDOC-936), 1997.
- Defence in Depth in Nuclear Safety (INSAG Series No. 10), 1996.
- Living probabilistic Safety Assessment (LPSA) (IAEA-TECDOC-1106, 1999.
- Framework for a Quality Assurance Program for Probabilistic Safety Assessment, (IAEA-TECDOC-1101), 1999.

## 2. General texts and basic sources for risk and reliability assessment

- “What Every Engineer should Know about Risk and Reliability Analysis”, M. Modarres, Marcel Dekker, Inc., 1993.

- “Reliability and Risk Analysis, Methods and Nuclear Power Applications”, Norman J. McCormick, Academic Press, 1981.

- “Determining Risks to Health, Federal Policy and Practice”, U.S. Department of Health and Human Services, Auburn House, 1986.

- *“Fault Tree Handbook”*, W.E. Vesely et al.,USNRC Report NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1981.

- *“Risk Assessment Handbook”*, Idaho National Engineering Laboratory, EG&G, SSRE-9300, September, 1990.

- “What Probabilistic Risk Assessment in the Nuclear Power Industry: Fundamentals and Applications”, R.R. Fulwood and R.E. Hall,, Pergamon Press, New York, 1988

- “Nuclear Power Plant Response to Severe Accidents, IDCOR Technical Summary Report”, Technology for Energy Corp., U.S. Atomic Industrial Forum, November 1984.

- “Integrated Approach Methodology: A Handbook for Power Plant Assessment", M. L. Roush, M. Modarres, R. N. M. Hunt, D. Kreps, R. Pierce Sandia National Laboratories, Contractor Report SAND87-7138 October 1987.

- “PRA Procedures Guide”, J.W. Hickman et al., USNRC Report NUREG/CR-2300 vols. 1 & 2, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1983.
  “Analysis of Core Damage Frequency: Internal Events Methodology”, D.M. Ericson, Jr. et al., USNRC Report NUREG/CR-4550 vol. 1, Rev. 1, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1990.

- “Evaluation of Severe Accident Risks: Methodology for the Accident Progression, Source Term, Consequence, and Risk Integration and Uncertainty Analysis”, E. Gorham-Bergeron et al., USNRC Report NUREG/CR-4551, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1990.

- “Recommended Procedures for External Event Risk Analyses for NUREG-1150", M.P. Bohm and J.A. Lambright USNRC Report NUREG/CR-4840, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1989.

- “Interim Reliability Evaluation Program Procedures Guide”, D.D. Carlson et al., USNRC Report NUREG/CR-2728, U.S. Nuclear Regulatory Commission, Washington, DC 2055, 1983.

- “Uncertainty in Risk Assessment, Risk Management and Decision Making”, Ed. V. Covello et al., Plenum Press, 1987.

- “Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Power Plants”, United States Regulatory Commission, WASH-1400 (NUREG-75/014), October, 1975.

### 2.1. General sources for PSA applications

- “Individual Plant Examination: Submittal Guidance”, USNRC, NUREG-1335, August 1989.

- “Applications of Probabilistic Risk Assessment”, Yankee Atomic Electric Company, EPRI report NP-7315, May 1991
- “Final PSA Applications Guide” (NUMARC/NEI)
- “Developing a Living Schedule, Fundamental Concepts”, Delian Corp., Nuclear Safety Analysis Center report, NSAC-90, August 1985.

### 2.2. Papers and articles

- *“The Practice of Zoning; How PRAs Can Be Used as a Decision-Making Tool in City and Regional Planning”*, M.F. Versteeg, Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 91-97.
- *"The Seveso Directive in the Netherlands; The Requirement for Chemical Industries to Submit an External Safety Report Including a PRA,"*M.F. Versteeg, Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, Pittsburgh, PA, 1989, pp 71-76.
- *"Performing a Plant Specific PRA by Hand -a Practical Reality",*R. Niall M. Hunt, M. Modarres, 1987 INTER-RAM Conference, Toronto, May 1987.
- *"The Routine Use of PRA in the Evaluation of Nuclear Plant Modifications",* R. Niall M. Hunt, 1986 Joint ANS/ASME Nuclear Power Conference Philadelphia, July 1986.
- *"Using 'GO' to Routinely Evaluate the Risk Significance of Nuclear Plant System Inter-actions",* R. Niall M. Hunt, Presented at the 1985 INTER-RAM Conference, Baltimore, April 1985.
- *"Use of a Plant Level Logic Model for Quantitative Assessment of some Experienced Systems Interaction",* B. B. Chu, D. C. Rees, L. J. Kripps, R. Niall M. Hunt, Melissa Bradley, 1985 ASME Winter Annual Meeting Miami Beach, November 1985.
- *"PRA -A Pragmatic Tool for Utility Risk Management?"*, R. Niall M. Hunt, International ANS/ENS Topical Meeting, Probabilistic Safety Methods and Applications, San Francisco, February 1985.
- *"Integrated Economic Risk Management in a Nuclear Power Plant"*, R. Niall M. Hunt, Mohammed Modarres, Society for Risk Analysis, Annual Meeting in Knoxville, October, 1984.

## 3. Reliability, availability and maintainability analysis

### 3.1. General texts and basic sources for reliability, availability and maintainability analysis

- *“Maintainability Assessment Methods and Enhancement Strategies for Nuclear and Fossil Fuel Power Plants,”* Lockheed Missiles and Space Company, EPRI Report NP-3588, July 1984.
- *“Guidelines for Availability Engineering as Applied to New Plant Design”*, EEI Availability Engineering Task Force, Edison Electric Institute, December 1983.
- *“Guidelines for Availability Engineering as Applied to Operating Plants”*, EEI Availability Engineering Task Force, Edison Electric Institute, December 1983.

- *"Power Plant Availability Engineering: Methods of Analysis, Program Planning, and Applications"*, Pickard, Lowe and Garrick, Electric Power Research Institute (EPRI) Report, NP-2168, May 1982.
- *"Review of the Analytical Methods for the Improvement of Nuclear Power Availability"*, Westinghouse Corp., EPRI report NP-1334, January 1980.

## 3.2. Papers and articles on RAM analysis

- *"RAM Methodology Selection"*, R. Niall M. Hunt, Thomas E. Wierman 17th INTER-RAM Conference for the Electric Power Industry, Hershey, Pennsylvania, June, 1990.
- *"Improving the Performance of Critical Plant Components - an Analytical Approach",* R. Niall M. Hunt, 1986 INTER-RAM Reliability Conference for the Electric Power Industry, Syracuse, June 1986.
- *"An Integral Approach to Analysis of Potential Plant Improvements",* Mohammed Modarres, Marvin Roush, R. Niall M. Hunt, R. Pearce Proceedings, American Power Conference Chicago, April 1986.
- *"Application of Goal Trees for Nuclear Power Plant Hardware Protection",* Mohammed Modarres, Marvin Roush, R. Niall M. Hunt, 8th International Conference on Structural Mechanics in Reactor Technology Brussels, Belgium, August 1985.
- *"Equivalent Availability Analysis as an Integral part of a Nuclear Plant Productivity Improvement Program"*, R. Niall M. Hunt, ASME Winter Annual Meeting Miami Beach, November 1985.
- *"Use of the Goal Tree Methodology to Evaluate Institutional Practices and their Effect on Power Plant Hardware Performance",* R. Niall M. Hunt, Marvin Roush, Mohammed Modarres, 1985 INTER-RAM Conference, Baltimore, April 1985.
- *"Application of Goal Trees in Reliability Allocation for Systems and Components of Nuclear Power Plants",* Mohammed Modarres, Marvin Roush, R. Niall M. Hunt, Presented at the 1985 INTER-RAM Conference, Baltimore, April 1985.
- *"Selection of Availability Analysis Techniques",* R. Niall M. Hunt, 1984 Reliability Conference for the Utility Industry, Las Vegas, Nevada, April 1984.

## 4. General texts and basic sources for PRA documentation and review

- *"IPERS guidelines for the International Peer Review Service"*, IAEA-TECDOC-XXX, March 1995.
- *"An Intensive Peer Review for Probabilistic Risk Assessment"*, Delian Corp., Nuclear Safety Analysis Center (EPRI) Report NSAC-67
- *"Documentation Design for Probabilistic Risk Assessment"*, Wood-Leaver and Assocs., EPRI Report, NP-3470, June 1984.

## 5. General texts and basic sources for risk or performance based plant technical specifications

- *"Handbook of Methods for Risk-Based Analyses of Technical Specifications"*, NUREG/CR-6141, I. S. Kim et al., Brookhaven National Laboratory, Avaplan Oy, SAIC, 1994,
- *"Risk Based Evaluation of Technical Specifications"*, Battelle Columbus, Electric Power Research Institute (EPRI) Interim Report NP-4317, December 1985

## 6. Plant Information Systems and Human Reliability Assessment

- *"Risk Sensitivity to Human Error"*, P. Samata et al., Brookhaven National Laboratory, NUREG/CR-5319.
- *"Accident Sequence Evaluation Procedure Program Human Reliability Analysis Procedure"*, Alan D. Swain, Sandia National Laboratories, NUREG/CR-4772, February 1987.
- *"Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP)"*, Weston, Whitehead and Graves, Sandia National Laboratory, NUREG/CR-4834, Vols 1 and 2, June 1987.
- *"Human Factors Guide for Nuclear Power Plant Control Room Development"*, Essex Corp., EPRI Report NP-3659.
- *"Systematic Human Action Reliability Procedure (SHARP)*, NUS Corp., EPRI Report NP-3583, June 1984.
- *"A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants"*, B.J. Bell, A.D. Swain, Sandia National Laboratories, NUREG/CR-2254, May 1983.
- *"Handbook of Human reliability Analysis with Emphasis on Nuclear Power Plant Applications"*, A.D. Swain, H.E. Goodman, Sandia National Laboratories USNRC, NUREG/CR-1278, 1983.
- *"Evaluation Criteria for Detailed Control Room Design Review"*, USNRC, NUREG-0801, October 1981.
- *"Human Detection and Diagnosis of System Failures, (NATO Conference Series)*", ed. J. Rasmussen and W. B. Rouse, Plenum Press, 1981.

### a. Papers and articles

- *"The Integrated Approach Methodology for Operator Information Evaluation",* R. Niall M. Hunt, Mohammed Modarres, R. Pearce, K. Stroube 1986 ANS/ENS Topical Conference on Human Factors Knoxville, April 1986.
- *"GOALTRES: An Expert System for Fault Detection and Analysis",* D. Chung, M. Modarres, R. N. M. Hunt, Reliability Engineering and System Safety.
- *"Application of an LWR Operator Information Systems Analysis to the Calvert Cliffs Nuclear Power Plant -Unit 1"* (DOE, ALO -1023), Marvin Roush, Joseph Braun, Niall Hunt, et al.

- *"Probabilistic Risk Assessment: A Look at the Role of Artificial Intelligence",* J. Wang, M. Modarres, R. N. M. Hunt, Nuclear Engineering and Design.

- *"Application of Goal Trees to Evaluation of the Impact of Information upon Plant Availability"*, Marvin L. Roush, Mohammed Modarres, Niall Hunt, International ANS/ENS Topical Meeting, Probabilistic Safety Methods & Applications, San Francisco, February 1985.

## • 7. Databases and data analysis

*Reliability Data Base, IAEA Compilation of Generic Component Reliability Data.*

- *IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Data for Nuclear Power Generating Stations, IEEE-Std. 500 1983 (Corrected Edition 1993).*
- *EPRI ALWR Reliability Data Base.*
- *"Reliability Data Book for Components in Swedish Nuclear Power Plants",* J.P. Bento,, Report No. RSK 85-25, Nuclear Safety Board of the Swedish Utilities for Swedish Nuclear Power Directorate, Sweden.
- *"Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessments"*, D.P. Mackowiak et al., USNRC Report NUREG/CR-3862, U.S. Nuclear Regulatory Commission, Washington, DC 20555, 1985.

### 7.1. Papers and articles

- *"The Use of Probabilistic Techniques to Assess Reactor Coolant Pump Motor Failure Rates",* R. A. Buttner, R. N. M. Hunt, ANS/ENS International Conference on Reactor Operations, Chicago, August 1987.

## 8. Aging risk assessment

The following provide some insights into the research performed to date in the area of Aging Risk Assessment:

- NUREG-1362, USNRC

- *"Evaluations of Core Melt Frequency Effects Due to Component Aging and Maintenance"*, W. Vesely et al., NUREG/CR-5510.

- *"Improved Eddy Current Inspection for Steam Generator Tubing"*, C.V. Dodd, et al. NUREG/CR-5478.

- *" Pressurized-Water Reactor Internals Aging Degradation Study"*, NUREG/CR-6048,, K.H. Luk.

- *"Guidelines for In-Service Testing at Nuclear Power Plants"*, USNRC NUREG-1482.

- *"Risk-Based Inspection - Development of Guidelines"*, ASME, NUREG/GR-0005. Vol 2, Part 1.

- *"Aging Assessment of Component Cooling Water Systems in Pressurized Water Reactors",* R. Lofaro, et al., NUREG/CR-5693.

- *"Aging of Nuclear Station Diesel Generators: Evaluation of Operating and Expert Experience"*, K.R. Hoopingarner, et al., NUREG/CR-4590.
- *"An Aging Assessment of Relays and Circuit Breakers and System Interactions"*, Franklin Research Center, NUREG/CR-4715.
- *"Comprehensive Aging Assessment of Circuit Breakers and Relays",* J. F. Gleason, NUREG/CR-5762.
- *"Aging and Service Wear of Solenoid Operated Valves Used in Safety Systems of Nuclear Power Plants"*, R. C. Kryter, NUREG/CR-4819.
- *"A Characterization of Check Valve Degradation and Failure"*, NUREG/CR-5944.

## 9. Root cause analysis

### 9.1. General texts and basic sources for root cause investigation

- *"Guidelines for Process Safety Incident Investigation",* AIChE Center for Chemical Process Safety (CCPS), 1993.
- *"The New Rational Manager"*, C.H. Kepner, B.B.Tregoe, Princeton Research Press, 1981.
- *"Management Oversight and Risk Tree (MORT)"* process:
  - ➢ *"The MORT User's Manual"*, R.W. Eicher, N.W. Knox, DOE 76-45/4, SSDC-4, Revision 2, May 1983.
  - ➢ *"Applications of MORT to Review of Safety Analyses"*, G.J. Briscoe et al.,DOE 76-45/17, SSDC-17 July 1979.
- *"Human Performance Evaluation System (HPES)"*, Institute for Nuclear Power Plant Operations (INPO), Marietta, GA.
- *"HSYS, A Methodology for Analyzing Human Performance in Operational Settings*", J.Harbour, S. Hill, Idaho National Engineering Laboratory, Draft: EGG-HFRU-8806.

### 9.2. Papers and articles

- "*GOALTRES: An Expert System for Fault Detection and Analysis",* D. Chung, M. Modarres, R. N. M. Hunt, Reliability Engineering and System Safety,
- *"Development of a Root Cause Analysis Workstation and its Application in Identifying the Cause of Reactor Scrams",* R. N. M. Hunt, M. A. Danner, M. Modarres, D. Chung ASME/ANS Joint Meeting, Myrtle Beach SC, April 1988.
- "A Knowledge Based Approach to Root Cause Failure Analysis", Su Chen, Modarres, Hunt and Danner, EPRI AI Conference, May, 1989, Orlando, Florida.
- *"Development of a Root Cause Analysis Workstation and its Application",* R. N. M. Hunt, M. A. Danner, M. Modarres, D. Chung, 15th INTER-Ram Conference, Portland OR, June 1988.

*"A Model-based Approach to on-line Process Disturbance Management, The Models"*. Reliability Engineering and System Safety, 28 (1990) pp. 265 -305, I.S. Kim, M. Modarres and R.N.M. Hunt.

- *"A Model-based Approach to On-line Process Disturbance Management, The Application"*. Reliability Engineering and System Safety, 29, (1990) pp. 185 -239, I.S. Kim, M. Modarres and R.N.M. Hunt.
- *"Toward the Practical Use of Expert System Technique for Process Disturbance Management"*. Reliability Engineering and System Safety, 28, (1990) pp. 307 -317, I.S. Kim, M. Modarres and R.N.M. Hunt.
- *"Common Cause Failure of Motor Operated Valves at the Washington Nuclear Plant 2"*, L.T. Pong, R. Niall M. Hunt, ANS International Topical Meeting, Seattle, September 1995.

## 10. Publications for advanced light water reactors

- *“Forging an International Industrial Concensus on Safety Standards for Future Light Water Reactor Power Plants”*, P. Bacher, K. Iida J. Taylor, World Energy Council, Tokyo, October 8-13, 1995.
- *“Advanced Light Water Reactor Utility Requirements Document”*, Vols. 1, 2 and 3, EPRI Report NP-6780-L, Palo Alto, California, September 1990.
- *“Projected Cost of Electricity for Major Alternatives to Future Nuclear Power Plants”,* EPRI ALWR Program Report**,** September 1995.
- *“European Utility Requirements for LWR Nuclear Power Plants”*, Rev. B, 1995.
- *“ Top Tier Requirements for KNGR”*, S.J. Cho, K. Lee, D. W. Jerng, TOPNOX International Conference, Volume 1, Paris, 1996.

## ABBREVIATIONS

| | |
|---|---|
| ABWR | advanced boiling water reactor |
| AC | alternating current |
| ADV | atmospheric dump valve |
| AFW | auxiliary feedwater |
| AIP | availability improvement programme |
| ALWR | advanced light water reactor |
| ATWS | anticipated transient without SCRAM |
| BWR | boiling water reactor |
| CCDF | complementary cumulative distribution function |
| CCF | common cause failure |
| CCFP | conditional containment failure probability |
| CCW | component cooling water |
| CDF | core damage frequency |
| CEA | control element assembly |
| CVCS | chemical and volume control system |
| DBA | design basis accident |
| DC | direct current |
| DCH | direct containment heating |
| DHR | decay heat removal system |
| D-RAP | design reliability assurance programme |
| EA | equivalent availability |
| EALWR | evolutionary advanced light water reactor |
| ECCS | emergency core cooling system |
| EPZ | emergency planning zone |
| ESD | event sequence diagram |
| ESFAS | engineered safeguards actuation system |
| EU | equivalent unavailability |
| FMEA | failure modes and effects analysis |
| FMECA | failure modes, effects and criticality analysis |
| FO | forced outage |
| FOR | forced outage rate |
| FR | forced reduction |
| FSAR | final safety analysis report |
| GQA | graded quality assurance |
| HCR | human cognitive response |
| HPCS | high pressure core spray |
| HPSI | high pressure safety injection |
| HPSR | high pressure safety injection (recirculation mode) |
| HRA | human reliability analysis |

| | |
|---|---|
| HVAC | heating, ventilation and air conditioning |
| IE | initiating event |
| ISA | integrated safety assessment |
| ISI | in-service inspection |
| IST | in-service test |
| LLOCA | large loss of coolant accident |
| LOCA | loss of coolant accident |
| LOSP | loss of offset power |
| LPSI | low pressure safety injection |
| MDC | maximum dependable capability |
| MFW | main feedwater |
| MLOCA | medium loss of coolant accident |
| MMI | man–machine interface |
| MO | maintenance outage |
| MOR | maintenance outage rate |
| MSSV | main steam safety valve |
| O-RAP | operations reliability assurance programme |
| PO | planned outage |
| POR | planned outage rate |
| PORV | pilot operated relief valve |
| PPE | personal protective equipment |
| PRA | probabilistic risk assessment (analysis) |
| PSA | probabilistic safety assessment (analysis) |
| PSAR | preliminary safety analysis report |
| QA | quality assurance |
| QAP | quality assurance programme or quality assurance policy |
| RA | reliability assurance |
| RAM | reliability, availability and maintainability |
| RAMI | reliability, availability and maintainability improvement |
| RAP | reliability assurance programme |
| RBI | risk based inspection |
| RBI&T | risk based inspection and test |
| RBMS | risk based management system |
| RCA | root cause analysis |
| RCIC | reactor cooling isolation condenser |
| RCM | reliability centered maintenance |
| RCP | reactor coolant pump |
| RCS | reactor coolant system |
| RMS | radiation monitoring system |
| RPS | reactor protection system |
| RRS | reactor regulating system |

| | |
|---|---|
| SA | safety analysis |
| SAR | safety analysis report |
| SCRAM | reactor trip |
| SHARP | systematic human actions reliability procedure |
| SGTR | steam generator tube rupture |
| SIT | safety injection tank |
| SLOCA | small loss of coolant accident |
| SRW | service water cooling system |
| SSC | system, structure or component |
| STP | surveillance test procedure |
| SWC | salt water cooling system |
| SWGR | switchgear |
| TBCCW | turbine building cooling water system |
| THERP | technique for human error rate prediction |
| USAR | updated safety analysis report |
| WASH-1400 | reactor safety study |

## CONTRIBUTORS TO DRAFTING AND REVIEW

| | |
|---|---|
| Andreani, M. | ENEL, Italy |
| Attalo, D. | Usina Nuclear de Angra 1, Brazil |
| Bjoere, S. | ABB Atom AB, Sweden |
| Balfanz, H.P. | Technischer Ueberwachungs-Verein Nord e.V., Germany |
| Board, J. | Nuclear Electric plc, United Kingdom |
| Choi, Young Sang | Korea Electric Power Research Institute, Republic of Korea |
| Cho, Byung Oke | International Atomic Energy Agency |
| Fukuda, M. | Nuclear Power Engineering Corporation, Japan |
| Gomez-Cobo, A. | International Atomic Energy Agency |
| Gubler, R. | International Atomic Energy Agency |
| Hunt, R. | SCIENTECH, Inc., United States of America |
| Kim, Yang-Eun | International Atomic Energy Agency |
| Lee, Boem-Su | KOPEC, Republic of Korea |
| Lienard, M. | TRACTEBEL Energy Engineering, Belgium |
| Na, Jang-Hwan | Korea Electric Power Research Institute, Republic of Korea |
| Niall M. | SCIENTECH, Inc., United States of America |
| Park, Sang Doug | Korea Electric Power Research Institute, Republic of Korea |
| Suh, Doo Suk | International Atomic Energy Agency |
| Trampus, P. | International Atomic Energy Agency |
| Yoo, Kyung Yeong | Korea Electric Power Research Institute, Republic of Korea |
| Zwingelstein, G. | Elictricité de France, France |

### Consultants Meetings

Vienna, Austria: 9–11 October 1995, 14–16 May 1996,
7–10 April 1997, 7–10 October 1997, 7–10 October 1997