Westinghouse Technology Systems Manual

Section 1.4

Introduction to Probabilistic Risk Assessment

TABLE OF CONTENTS

LIST OF FIGURES

1.4 INTRODUCTION TO PROBABILISTIC RISK ASSESSMENT

Learning Objectives:

1. Define the term risk.

2. List the three questions that a plant PRA answers.

3. Describe the different levels of PRA.

4. Define the terms: internal and external initiating event, accident sequence, plant damage state, front-line system, and support system.

5. Explain why event tree analysis is performed and the important features of an event tree.

6. Explain why fault tree analysis is performed and the four types of faults included in the fault trees.

7. List the four types of accident sequences that are important.

8. Identify how importance measures can be used in risk management.

9. List three regulatory uses of PRA.

10. List two utility uses of PRA.

11. Identify two possible uses of PRA information for plant inspectors.

1.4.1 Introduction

There are many definitions of risk. However, most of them include two basic factors: likelihood and consequences. Therefore, for the purpose of nuclear power plant safety assessments, risk is defined as the likelihood and consequences of potential accidents at commercial nuclear power plants.

A Probabilistic Risk Assessment (PRA) is an engineering tool used to quantify the risk of a facility. PRA is used primarily to address the likelihood and consequences of rare events at nuclear power plants. These events are generally referred to as severe accidents. The PRA augments traditional engineering analyses by providing quantitative measures of safety and thus a means of addressing the relative significance of issues in relation to plant safety. Basically, a nuclear power plant PRA answers three questions:

- What can go wrong?
- How likely is it?
- What are the consequences?

Probabilistic risk assessment is a multi-disciplinary approach employing various methods including system reliability, containment response, and fission release and public consequence analyses. PRA treats the entire plant and its constituent systems in an integrated fashion. Because of this, subtle interrelationships can be discovered that are important to risk. Another important attribute of the PRA method is it involves both single and multiple failure analysis. Multiple failures often lead to situations beyond system design basis and, in some cases, are more likely than single failures. By addressing multiple failures, the PRA can cover a broad spectrum of potential accidents at plants.

1.4.2 History and Background

The first comprehensive development and application of PRA techniques in the commercial nuclear power industry was the NRC sponsored Reactor Safety Study (RSS). The RSS analyzed both a BWR (Peach Bottom) and PWR (Surry). The report of the RSS results (1), generally referred to as WASH-1400, was published in October of 1975. The basic PRA approach developed by the RSS is still used today.

The principal objective of the RSS was to quantify the risk to the public from U.S. commercial nuclear power plants. Because it was the first broad scale application of event and fault tree methods to a system as complex as a nuclear power plant; analyzed conditions beyond the design basis; and attempted to quantify the risk; it was one of the more controversial documents in the history of reactor safety.

A group called the Lewis Committee performed a peer review on the RSS and published a report (2), NUREG/CR-0400, to the U.S. Nuclear Regulatory Commission three years later to describe the effect of the RSS results on the regulatory process. The report concluded that although the RSS had some flaws and PRA had not been formally used in the licensing process, PRA methods were the best available and should be used to assist in the allocation of the limited resources available for the improvement of safety.

The 1979 accident at Three Mile Island (TMI) substantially changed the character of the NRC's regulatory system. The accident revealed that perhaps nuclear reactors might not be safe enough and that new policies and approaches were required. Based on comments and recommendation from the Kemeny and Rogovin investigations (3) of the TMI accident, a substantial research program on severe accident phenomenology was initiated (e.g., those accidents beyond the design basis which could result in core damage). It was also recommended that PRA be used more by the staff to complement its traditional, non-probabilistic methods of analyzing nuclear plant safety. Rogovin also suggested in a report (4) to the Commissioners and the public, NUREG/CR-1250, that the NRC policy on severe accidents consider 1) more severe accidents in the licensing process and 2) probabilistic safety goals to help define what is an acceptable level of plant safety.

Soon thereafter, the NRC staff sponsored the Interim Reliability Evaluation Program (5), a series of plant reliability studies reported in NUREG/CR-2728, to develop methods for the efficient use of PRA to analyze the various designs of operating

reactors and to increase the cadre of experienced PRA practitioners. By the mid 1980's, general procedures for performing PRAs were developed and documented in the PRA Procedures Guide (6), NUREG/CR-2300. The current status of PRA, its relationship to the nuclear regulatory process, and a summary of PRA perspectives available at that time (1984) was published in the Probabilistic Risk Assessment Reference Document (7), NUREG-1050. This document also discussed the potential uses of PRA results for regulatory purposes.

In the late 1980, the U.S. Nuclear Regulatory Commission sponsored a current assessment of severe accident risks for five commercial nuclear power plants in a report called Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants (8), NUREG-1150. This report included an update of the RSS risk assessments of Surry and Peach Bottom and provided the latest NRC version of the state of the art in PRA models, methods, and approaches. The results were to be used to support prioritization of safety issues.

Recently, the NRC issued a letter to initiate an Individual Plant Examination (IPE) Program for Severe Accident Vulnerabilities (9), Generic Letter No. 88-20. The NRC requested each licensed nuclear power plant to identify plant specific vulnerabilities to severe accidents by performance of a Level 1 PRA for internal events and limited Level 2 analysis or other equivalent, approved means. The various levels of PRA analysis are described in section 1.4.3. The IPE letter is the main reason PRAs are being performed by utilities today.

A summary of the insights gained from previous risk assessments are as follows:

1. As illustrated by the NUREG-1150 results (8) and previous plant PRAs, the PRAs reflect details of plant systems, operation and physical lay out. Since nuclear power plants in the U.S. are not standardized, the PRA results are very plant specific. Reactor design, equipment, location, and operation (power level, testing and maintenance, operator actions) have a large impact on the outcome. Therefore, in detail, the results can differ significantly from plant to plant.

2. Even with the differences in the detailed results between plant studies, PRA can be used for some generic applications as listed in NUREG-1050 (7). Some examples are:

    - Regulatory activity prioritization,
    - Safety issue evaluation,
    - Resource allocation,
    - Inspection program prioritization, and
    - NRC policy development.

3. Using PRA in the decision process can show which changes are desirable to improve plant safety.

4. PRAs have also been used as a cost saving tool.

5. PRAs have pointed out some general differences with respect to BWRs and PWRs as a class. For example, NUREG-1150 (8) states that:

a. Principal accident contributor to core damage frequency:
   BWRs - station blackout and ATWS
   PWRs - loss of coolant accident

b. Core damage frequency:
   BWRs-lower than PWRs, due to more redundant systems
   PWRs -higher than BWRs, fewer ways to supply water to the reactor coolant system

c. Early containment failure given a core damage accident:
   BWRs -higher probability
   PWRs - lower probability, due to stronger and larger containments

The major contributors to core damage by accident type for the NUREG-1150 PWR and BWR plants are shown in Figure 1.4-1.

1.4.3 Levels of PRA

A full scope PRA, calculating the risk to the public, involves three discrete levels of study. Figure 1.4-2 illustrates the activities and/or products associated with each level. The outputs of the three levels are as follows:

- Level 1 - plant systems modeling which computes the frequency of core damage;
- Level 2 - accident phenomenology and fission product transport analysis which computes the inventories of fission products released to the environment (source terms) and their frequencies; and
- Level 3 - consequence analysis which computes the public health effects and their likelihood from the releases of fission products.

The Level 1 PRA involves modeling plant systems and calculating frequencies of the potential accidents that could result in core damage. To identify the potential accidents and quantify their frequency of occurrence, system safety analysis methods are used (e.g., event trees, fault trees) along with initiating event frequencies, component failure data, human error rates, and common cause failure data. From this level of the PRA, the accident sequences resulting in core damage are identified and the total core damage frequency is determined.

The Level 1 PRA results provide an important quantitative measure: Core Damage Frequency. This measure is useful in efforts to manage plant safety because it is directly related to the plant systems design and operation and an indicator of the potential risk to the facility, and indirectly the public, from potential accidents. Computation of how design and operational changes effect core damage frequency indirectly indicate the impact on plant safety. Therefore, the following discussion focuses primarily on the methodology and results of the Level 1 PRA.

A set of accident sequences is the principle product of the Level 1 PRA activities. An accident sequence is a postulated occurrence consisting of an initiating event or initiating event class and a specific combination of success and failure states of the

systems and/or operations which, if successful, mitigate the impact of the initiating event to maintain the plant in a safe and stable state.

Although the accident sequences of primary interest in a Level 1 lead to core damage, all these accident sequences are not equivalent. Some are more severe than others in terms of potential plant damage and/or public health consequences.

Therefore, all the Level 1 accident sequences are classified into plant damage states according to those factors which determine the potential severity of the sequences.

A Plant Damage State is a grouping of accident sequences that have the potential for similar outcomes in terms of containment response and fission product release. Characteristics of accident sequences such as reactor coolant system pressure, event timing, and system availability and operational status are considered in the development of the plant damage states. All the accident sequences with similar characteristics are put in the same plant damage state.

For example, accident sequences with containment safeguards systems failed would be put in different plant damage states from those with successful containment safeguards system operation and accident sequences with failure of emergency coolant injection put in different states than those with successful injection. Each plant damage state potentially results in a different challenge to the containment and ultimately a different inventory of fission products (source term) released to the environment.

The plant damage states define the important accident characteristics for use in the analysis of the containment response, behavior of the damaged core, and the transport of the fission products to the environment outside the containment. Therefore, the plant damage states provide the interface with the Level 2 and 3 PRA activities where the accident progression, containment response, fission product release, and subsequent risk to the public is calculated.

The output of the Level 1 PRA activities is generated principally by the use of the event tree and fault tree analysis methodology. A brief description of these methods and how they are used to determine core damage frequency is provided in the following sections.

The Level 2 PRA involves thermal hydraulic and structural analyses of containment, as well as modeling the behavior of fission products during the postulated accident. To develop and quantify these models, computer codes are utilized. From this level of the PRA, the magnitude, nature and frequency of radio nuclide releases are determined.

The Level 3 PRA involves calculating the health impact on the public from the release of the radio nuclides. To quantify the releases health effects, plume dispersion, weather characteristics (meteorology), population concentration, doses, and evacuation procedures are addressed. Computer codes are used to compute the consequences of the releases. From this level of the PRA, the number of early fatalities and delayed cancer fatalities are computed along with their likelihood.

1.4.4 Event Tree Analysis

The analytical technique used to identify accident sequences is called Event Tree Analysis. Event trees order and depict the success or failure of functions or systems required to mitigate the potential effects of an initiating event. An event tree is a simple diagram, similar to a decision tree, which merely illustrates the potential combinations of events which are of interest given some initial condition (initiating event).

To illustrate the technique, a simple event tree example has been provided. This event tree has been developed to examine the ways your instructor may fail to be here, first thing in the morning, to explain this to you.

The initiating event for this analysis is sunrise and we want to make sure that your instructor gets up and makes it to the classroom. The systems which are required to "operate" to assure that this happens are an alarm clock or wake-up call to get your instructor up, an automobile to get him or her to the building, and the elevator or the stairs to get him or her up here to the class room. The results of the event tree analysis for the instructor's failure to be in class are shown in Figure 1.4-3.

The combinations of "system" failures and successes, and the functions they perform, determine the status of the instructor (i.e., in class or absent). In event tree analysis, an upward branch (vertical line) represents a success of the system and a downward line represents a failure. Each unique combination of successes and failures is called an event tree sequence (or accident sequence). The sequences are identified by using the letters (or other identifier) corresponding to the initiating event and the systems that failed.

The sequences are developed by going through the event tree heading by heading and developing a success and failure path only in those cases where it has a bearing on the outcome (e.g., is the instructor in class or not?). Other cases which are not physically possible or do not impact the outcome are not developed. For example, when the alarm clock is successful, we do not postulate failure of the wake-up call because the instructor is already awake. Likewise, if the automobile fails, neither the elevator nor the stairs can get the instructor to class.

To demonstrate the fact that all sequences are not equal, compare sequences IAC and IAB. In IAC, the instructor is awake, but never arrives in class because either the car fails or he or she is stuck, fuming, in traffic. However, in sequence IAB, both the alarm clock and wake-up call fail to wake the instructor and he or she remains in bed sleeping (hopefully with pleasant dreams). Clearly, the effects on the instructor of these two sequences are drastically different.

For nuclear power plants, systemic event trees (event trees with systems as headings) display the combinations of plant system failures that can result in core damage. They are constructed for each initiating event group. An individual path through such an event tree (an accident sequence) identifies specific combinations of system successes and failures leading to (or avoiding) core damage. As such, the event tree qualitatively identifies what must fail in a plant in order to cause core damage.

Most initiating events for nuclear plant PRAs are those events that occur while the reactor is operating at full power, trip the plant, and require the operation of various systems to bring the reactor to a safe, stable state. Some PRAs are just starting to look at initiating events while the reactor is in other modes of operation and at events that involve the fuel storage pool. All initiating events applicable to the particular plant being analyzed must be identified along with their associated frequencies. These initiating events are collected into groups for performance of the event tree analysis.

The two kinds of initiating events considered in PRAs are:

1. Internal initiating events are those that occur mainly within the bounds of the systems being analyzed. Examples include: loss of coolant accidents, loss of offsite power, turbine trips and loss of feedwater events.

2. External initiating events are those events that generally occur outside the systems being modeled. Some examples are earthquakes, fires, and floods.

Most PRAs to date include only an analysis of internal events.

In general, a separate event tree will be developed for each initiating event group. Identification of these initiating event groups is based upon the unique combinations of mitigating systems and success criteria. For example, NUREG/CR-4550 (11) lists BWR and PWR generic transient classifications along with their associated frequencies. Specifically, two initiating event groups (or classes) for transients are identified:

1. Transients with Power Conversion System (PCS) available, and

2. Transients with loss of PCS.

This differentiation is made because if the PCS (i.e., main feedwater) is available, it can be used as a heat sink; therefore, events that could result in a plant trip with PCS available have different mitigating systems initially available than in the case with PCS unavailable.

The headings listed across the top of an event tree consist of those systems that mitigate the impact of the initiating event, (e.g., decay heat removal, coolant makeup systems, etc.). The required mitigating systems, referred to as front line systems in the PRA, will be identified for each initiating event. Front line systems are those systems that can perform the required safety (mitigating) functions for the initiating events or event groups. Specific success criteria, for each front line system that performs a mitigating (safety) function, must be identified. In addition to a performance definition (e.g., flow rate, response time, trip limits), these success criteria must be stated in discrete hardware terms, such as the number of required pumps, flow paths, instrument trains, or power buses. Ultimately, the success criteria for each front line system will be based on detailed thermal-hydraulic, core physics, or other phenomenological calculations.

1.4.5 Systems Analysis

The event tree analysis identifies the accident sequences that can result in core damage. Each of these sequences consists of a specific combination of an initiating event class and front line (mitigating) system failures. To identify how the systems might fail, system modeling is performed.

The most common analytical technique used to model system failures is fault tree analysis. Other modeling techniques such as expressing failure in the form of an equation or using a single failure probability number, referred to as a 'black box' model, can be used for those systems which are relatively simple and/or whose failures are independent from the other systems being analyzed. In some cases, the complexity of the system and the availability of failure data may warrant the use of data rather than a model (e.g., the main feedwater system failure is often represented by a 'black box' model).

Formally, fault tree analysis can be defined as: "an analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety standpoint), and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur" NUREG-0492 (12).

In other words, the fault tree is a technique to identify the ways in which a system may fail to perform its intended function. The fault tree is constructed using rules and logic symbols. It develops the ways in which a system can fail by identifying all credible single and multiple failures. The result is a logic diagram of system faults which can be evaluated by a computer.

As an example of a fault tree, let us select the alarm clock from our event tree example in section 1.4.4. We are interested in how the alarm clock can fail to operate at sunrise. Therefore, we will develop a fault tree for the following event from the event tree: "Alarm clock fails to operate at sunrise". Figure 1.4-4 shows the start of this fault tree.

As shown in this figure, the alarm clock will fail to operate if one or more of the following fault events occur:

1. No power available to the buzzer,

2. Buzzer not commanded to buzz at sunrise, or

3. Buzzer fails.

Since the alarm clock will fail if only the buzzer fails, that fault by itself is a minimal cut set for this fault tree. While the alarm clock will also fail if both the buzzer fails and there is a loss of offsite power, this condition is more than the minimum, necessary, and sufficient set of faults and is not a minimal cut set.

If we were to complete the example fault tree, the events "no power available to the buzzer at sunrise" and "buzzer not commanded to buzz at sunrise" would both be

developed further. The fault tree development continues until we have a tree which ends in events for which we have or can develop failure probability data and the interactions and dependencies between systems are properly addressed.

The purpose of fault tree analysis is to identify the ways in which a system can fail and provide a means to find system dependencies and subtle interactions that can contribute to multiple system failures. Fault trees are used to determine the minimal cut sets for system failure and accident sequences. The minimum, necessary, and sufficient sets of events which could result in system failure or an accident sequence are called minimal cut sets.

The fault tree includes only those fault events and logical interrelationships that contribute to the system failure identified in the event tree. Fault tree analysis is done for the front line systems and all the systems that supply required services (e.g., component cooling, AC power, or HVAC) to the front line systems. This latter type of system is referred to as a support system in the PRA. Support systems can also provide required services to other support systems (e.g., HVAC in an AC power switch gear room). Fault trees for the support systems include fault events of the systems which provide these required services.

There are generally four types of faults considered in system models. These fault events are

- Hardware failures,
- Test and maintenance errors,
- Human errors, and
- Dependent failures.

The dependent failures include faults as a result of support system failures and common cause failure of multiple components.

1.4.6 Accident Sequence Evaluation

For the Level 1 PRA, the accident sequences of interest for the evaluation process are those that are the most likely and/or potentially the most severe. The accident sequences are evaluated by computer to determine:

1. How they might occur in terms of the faults identified in the system models (qualitative results), and

2. Their frequency of occurrence (quantitative results).

This evaluation is done for internal events by combining the appropriate models for the system failure events with the initiating event group for each accident sequence. Likelihood data is assigned to each event in the models, including the initiating event group. This data comes from the analysis and data bases of:

- Component failure rates,
- Maintenance frequencies,

- Human error rates,
- Common cause failure probabilities, and
- Initiating event frequencies.

For external events, the evaluation includes definition of the frequency and severity of the external event (hazard function) and the impact of the external event on the likelihood of failure of the front line and support systems.

Methodologies employed in PRAs identify the minimum set of events that could cause an accident sequence resulting in core damage. These minimum, necessary sufficient sets of events are called minimal cut sets. Minimal cut sets identify the specific system failures, and maintenance and operational errors which combine to result in an accident leading to core damage. Each type of accident sequence can occur in many different ways and thus has many different minimal cut sets.

Each minimal cut set is quantified by identifying the probability of each system fault event and the frequency of the initiating event in the cut set. All cut set frequencies for an accident sequence are combined to obtain the total sequence frequency. Those minimal cut sets that contribute approximately 90% to 95% of the total sequence frequency are called dominant cut sets. The most dominant is that cut set which contributes itself the most to the total frequency.

The frequencies of all the core damage sequences are combined to calculate total core damage frequency. The set of sequences that contributes 90% to 95% of the total core damage frequency are referred to as dominant sequences. These sequences are often grouped by accident type based on the initiating event and some safety system failures.

1.4.6.1 Importance Measures

Based on the total core damage frequency and the frequency of the individual fault events, quantitative importance measures can be determined for the various accident sequences, systems, cut sets, and individual fault events. Three most often used importance measures are Percent Contribution, Risk Reduction, and Risk Achievement (or Risk Increase).

The Percent Contribution importance measure, as defined for an event or system, indicates the percent of the total core damage frequency which includes that event. Computing the percent contribution involves summing the frequencies of all cut sets that include the event or system of interest and dividing by the total core damage frequency. The percent contribution measure gives the percentage of the total core damage frequency associated with that event or system. Accident sequences, events or systems with a large percent contribution measure have the biggest contribution to the total core damage frequency. Because PRA includes the postulation of multiple failures, the total of the percent contribution measures often exceed 1.0. Figures 1.4-5 and 1.4-6 show the range of percent contributions for various BWR and PWR systems, respectively.

The Risk Reduction importance measure as defined for a system or event measures the sensitivity of the total core damage frequency to a decrease in the likelihood of

system failure or the event of interest. First, to obtain this measure, the failure frequency of the event of interest is reduced to zero. Then, the total core damage frequency is divided by the sum of all the cut set frequencies, with the event of interest frequency at zero. Preventing or limiting that event with the largest risk reduction value will have the greatest effect in decreasing the total core damage frequency. Therefore, the risk reduction importance measure shows where the most gain can be achieved on safety improvements (e.g., the greatest decrease in total core damage frequency). Figure 1.4-7 shows the range of risk reduction for Sequoyah Safety Systems.

The Risk Achievement (or Risk Increase) importance measure as defined for a system or event measures the sensitivity of the total core damage frequency to an increase in the likelihood of the event of interest. To obtain this measure, the frequency of the event of interest is set to one. Then, the cut set frequencies are summed and divided by the total core damage frequency. The risk achievement measure identifies those areas where it is most important to verify equipment is as reliable as assumed during the initial core damage frequency calculation. The largest risk achievement measure indicates the event that should be verified reliable because it has the greatest negative impact on the total core damage frequency (e.g., the greatest increase in total core damage frequency). Figure 1.4-7 shows the range of risk achievement for Sequoyah Safety Systems.

1.4.7 Information Obtained from PRA

As mentioned in Section 1.4.3, a PRA can be performed at various levels, depending on the objectives of the study. Each discrete level, Level 1, 2, and 3, provides different information. The ultimate result of a full scope, Level 3, PRA is quantification of the risk to the public (e.g., the likelihood and number of early and latent fatalities).

The Level 1 PRA results provide an important quantitative measure: core damage frequency. Generally, the total core damage frequency for a commercial nuclear power plant is in the range of $1x10^{-4}$ to $1x10^{-6}$ per reactor year.

The qualitative results of accident sequence evaluation gives insights on the behavior of system failures leading to core damage. Minimal cut sets for the accident sequences consisting of the initiator and faults from the system models are determined. These minimal cut sets represent the sets of fault events that must exist simultaneously for the accident sequence to occur.

The Level 1 PRA accident sequence results have been used extensively to investigate generic safety issues and play a major role in rule making. Some of the more notable examples of accidents addressed by PRA include:

- Station Blackout,
- Anticipated Transient Without Scram (ATWS),
- Failure of Long Term Heat Removal (RHR Failure), and
- Intersystem (or interfacing) LOCA.

A station blackout accident sequence consists of a loss of offsite power accompanied by a total loss of onsite emergency ac power. This impacts the availability of some of the front line systems which need to operate to achieve a safe, stable shutdown. The NRC requires that every utility provide their plans for response to station blackout. PRA evaluation of station blackout accidents at nuclear power plants is described in NUREG-1032 (13).

Anticipated transients without scram (ATWS) sequences consist of a transient which would normally result in reactor trip (scram) and a failure of the systems that scram the reactor. These sequences can result in large pressure and temperature transients in the reactor coolant system and containment. PRAs have shown these types of sequences to be significant, especially at BWRs. Early discussion of the probability of failure to scram can be found in NUREG-0480 (14). Cost-benefit analysis using PRA analysis and results was done extensively during the Anticipated Transient Without Scram (ATWS) rule making process.

The failure of long term decay heat removal (residual heat removal) after a loss of coolant accident (LOCA) is another potentially significant accident sequence, especially at PWRs. A significant PRA effort was sponsored by the NRC to examine this potential accident sequence and identify potential back fits to reduce the frequency of this accident. The results of a value impact study on decay heat removal concepts are documented in NUREG/CR-2883 (15).

The Reactor Safety Study (1) identified the inter-system LOCA as a significant accident sequence for the Surry plant. This accident consists of a LOCA which violates the containment pressure boundary as a result of high pressure NSSS coolant inadvertently flowing into a low pressure line outside the containment boundary. This type of accident sequence has a very low frequency but is potentially very severe because it bypasses the containment and results in the failure of emergency core cooling.

1.4.8 Uses of PRA

The PRA Reference Document (7), NUREG-1050, addresses the many uses of PRA both on a generic and plant specific basis. However, because each nuclear power plant is essentially unique, the most powerful uses of the PRA is as a plant specific tool. PRAs can be used in two basic ways to:

1. Support plant operations, maintenance, inspection, and planning activities; and

2. Provide information regarding changes to improve plant safety.

The PRA supports plant activities by providing information on the risk significant areas in plant operation, maintenance and design. Then operations, maintenance, inspection, and planning can appropriately address these areas to control the risk at acceptable levels.

The risk significant areas are identified by the results of the PRA. These areas are where the most attention and effort should be focused. Several risk significant

areas are: dominant contributors (indicate which failures are the largest contributors to the likelihood of accident sequences), dominant accident sequences (depict the failure paths that contribute most to core damage frequency), and importance measures (evaluate what contributes most to core damage, what would reduce the core damage frequency the most, and what has the greatest potential for increasing core damage frequency should it not be as reliable as desired).

The PRA results can be utilized in many ways during planning and operational activities of the nuclear plant. The results have an important role in risk management, training, emergency planning, maintenance planning, and risk based inspections.

1.4.8.1 Risk Management

Risk management is a means of prioritizing resources and concerns to control a level of safety. The PRA can be used during plant operation to prioritize operational and maintenance resources to maintain safety at acceptable levels. This is accomplished, in part, by periodically updating the PRA results to keep current with plant configuration and component failure. Importance measures can be used to indicate where preventive actions would be most beneficial and what is most important to maintain at acceptable safety levels. Based on the updated results, adjustments in plant activities and design can be made, as appropriate, to maintain the desired level of safety as indicated by the results of the PRA.

1.4.8.2 Operator Training and Simulator Design

Training can be emphasized for the operation of any system designated as risk significant in the PRA results. Operators can be trained on the dominant and/or most severe accident sequences identified by the PRA to improve human reliability for these situations. Assessments of instrumentation and status monitoring adequacy can be made to decrease human error rates.

1.4.8.3 Emergency Planning

Dominant accident sequences can be used to train emergency response personnel on what to expect in the event of a severe accident at a nuclear power plant. These sequences can also provide the basis for the development of guidelines for declaration of site and general emergencies. The PRA results and models can be used to aid in diagnosis and prognosis of accidents in progress.

1.4.8.4 Maintenance Planning

PRAs provide information to allow the concentration of maintenance efforts on the equipment associated with large risk achievement measures and reduce efforts in areas that have little impact on core damage. The impact on safety of potential changes to preventive and corrective maintenance practices can be measured to identify beneficial changes to improve safety.

1.4.8.5 Risk-Based Inspections

The PRA provides information on dominant accident sequences and their minimal cut sets. Some PRAs have already been used to design the risk based portion of plant inspection programs (16), NUREG/CR-5058. Inspection programs can be prioritized to address the minimization of hardware challenges, the assurance of hardware availability, and the effectiveness of plant staff actions as they relate to the systems and faults included in the dominant accident sequences.

PRA supports the assessment of plant changes by providing quantitative measures of the relative level of safety of each change. This is accomplished by performing sensitivity studies. A sensitivity study is a study of how different assumptions, configurations, data or other potential changes in the basis of the PRA impact the results.

1.4.8.6 Design Trade Studies

To analyze the impact of various proposed designs with respect to their quantitative impact on risk, the PRA is reevaluated for each different design. This provides a relative measure of the potential positive (or negative) impact each design will have with respect to plant risk due to severe accidents.

1.4.8.7 Backfit Decisions

There are many cases where PRAs have been used to support the back fit decision process. After the TMI accident several TMI action plan issues evolved. Consumers Power performed a PRA of the Big Rock Point nuclear power plant to assist in identifying those TMI generated changes which might actually have an impact on the risk at the plant. As a result, Consumers Power was able to negotiate exemptions on seven of the issues that did not significantly lower risk at Big Rock Point, saving over $45 million (7). In addition, Consumers Power used the PRA to identify changes necessary to reduce the core damage frequency at Big Rock Point to acceptable levels.

1.4.8.8 Procedural Changes

Changes to procedures are often recommended as a result of the PRA. For example, a PRA done on Arkansas Nuclear One identified several procedural changes to reduce the probability of core damage (7). One included staggering the quarterly tests on the station batteries to reduce the probability of common cause failures in the dc power supply.

1.4.8.9 Cost-benefit Analysis

By considering the cost of the changes analyzed by the PRA, a cost-benefit analysis can be accomplished. The cost of a change is generally considered to be the cost associated with it in dollars, including the cost of design, licensing, implementation, operation and maintenance. Sometimes the cost of replacement power is included for back fits requiring plant shut down to implement. The benefit of the change is the reduction in risk if the change is implemented. The most cost effective change

of all those that achieve acceptable safety, is the one which provides the most improvement in safety for the least cost. This type of cost-benefit analysis was done extensively during the Anticipated Transient Without Scram (ATWS) rule making process.

1.4.9 Inspection Effort

It is increasingly important to be familiar with PRA activities and results mainly because of the increased use of the results in plant operation and licensing. As mentioned, the NRC issued a letter to initiate an Individual Plant Examination (IPE) Program for Severe Accident Vulnerabilities (9). The NRC is requesting each licensed nuclear power plant to identify plant specific vulnerabilities to severe accidents by performance of a Level 1 PRA for internal events and limited Level 2 analysis or other equivalent, approved means.

As a plant inspector, you will be expected to use PRA results to assist in prioritizing your activities at the plant. NRC has used PRA information to support the activities of the operational assessment and readiness (OAR) team reviews of safety significant equipment and actions.

You will need to be alert for situations in the plant which constitute near misses. That is, you need to recognize those events that bring the plant close to an accident sequence occurrence. For example, the service water system (SWS) at a BWR was contaminated with silt. This increased the probability of common cause failure of the redundant valves in the SWS. Because the SWS is a support system for many other systems, this resulted in a significant increase in the likelihood of core damage at the plant. Recognizing the significance of events at the plant is especially true for those related to sequences such as ATWS and inter-system LOCA which can have severe consequences.

Finally, you will find yourself in more and more discussions where PRA results are being used or misused to justify a particular action or inaction. Therefore, it is important that you are familiar with the types of information a PRA provides and can use the PRA information accurately in your discussions and decisions.

1.4.10 Summary

PRA has become a part of the safety culture of both the NRC and the utilities. The IPE letter requires that every operating plant have a Level 1 PRA or equivalent.

The Level 1 PRA uses event trees to identify potential accident sequences that could result in core damage and fault trees to identify the system faults that can result in accident sequences. The event trees and the fault trees are used to determine:

1. How accident sequences might occur in terms of the faults identified in the system models (qualitative results), and

2. The frequency of occurrence (quantitative results).

By computing quantitative measures of risk, PRA provides the means to identify the relative importance of accident sequences, systems, and events to plant safety. Because of this characteristic of the PRA results, it is being widely used to assist in plant operations and planning, and to assess the impact of potential design and operational changes on plant safety.

Currently, the PRA methods and results are being used to assist the NRC in addressing potential nuclear power plant accident sequences of concern. Among these are station blackout, ATWS, failure of long term decay heat removal, and the inter-system (interfacing) LOCA.

1.4.11 References

1. "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", (WASH-1400) NUREG-75/014, U.S. Nuclear Regulatory Commission, Washington, DC, October 1975.

2. "Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission", NUREG/CR-0400, September 1978.

3. "Report of the President's Commission on the Accident at Three Mile Island", J.G. Kemeny et al., October 1979.

4. "Three Mile Island - A Report to the Commissioners and to the Public", NUREG/CR-1250, Vol. 1, January 1980.

5. "Interim Reliability Evaluation Program Procedures Guide", NUREG/CR- 2728, U.S. Nuclear Regulatory Commission, Washington, DC, January 1983.

6. "PRA Procedures Guide", NUREG/CR-2300, U.S. Nuclear Regulatory Commission, Washington, DC, January 1983.

7. "Probabilistic Risk Assessment Reference Document", NUREG-1050, U.S. Nuclear Regulatory Commission, Washington, DC, September 1984.

8. "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants", NUREG-1150, U.S. Nuclear Regulatory Commission, June 1989.

9. "Individual Plant Examination for Severe Accident Vulnerabilities", Generic Letter No. 88-20, U.S. Nuclear Regulatory Commission, Washington, DC, November 1988.

10. "Fundamentals of PRA", Idaho National Engineering Laboratory, Idaho Falls, ID, January 1990.

11. “Analysis of Core Damage Frequency: Internal Events Methodology”, NUREG/CR-4550, Vol. 1, Rev. 1, SAND86-2048, Sandia National Laboratories, Albuquerque, NM, January 1990.

12. “Fault Tree Handbook”, NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, DC, January 1981.

13. “Evaluation of Station Blackout Accidents at Nuclear Power Plants - Technical Findings Related to Unresolved Safety Issue A-44”, NUREG-1032, U.S. Nuclear Regulatory Commission, Washington, DC, June 1988.

14. “Anticipated Transients Without Scram for Light Water Reactors”, NUREG-0480, Vol. 1, U.S. Nuclear Regulatory Commission, Washington, DC, April 1978.

15. “Study of the Value and Impact of Alternative Decay Heat Removal Concepts for Light Water Reactors”, NUREG/CR-2883, Vol. 1,2,3, U.S. Nuclear Regulatory Commission, Washington, DC, June 1985.

16. “PRA Applications Program for Inspection at ANO-1”, NUREG/CR-5058, U.S. Nuclear Regulatory Commission, Washington, DC, March 1987

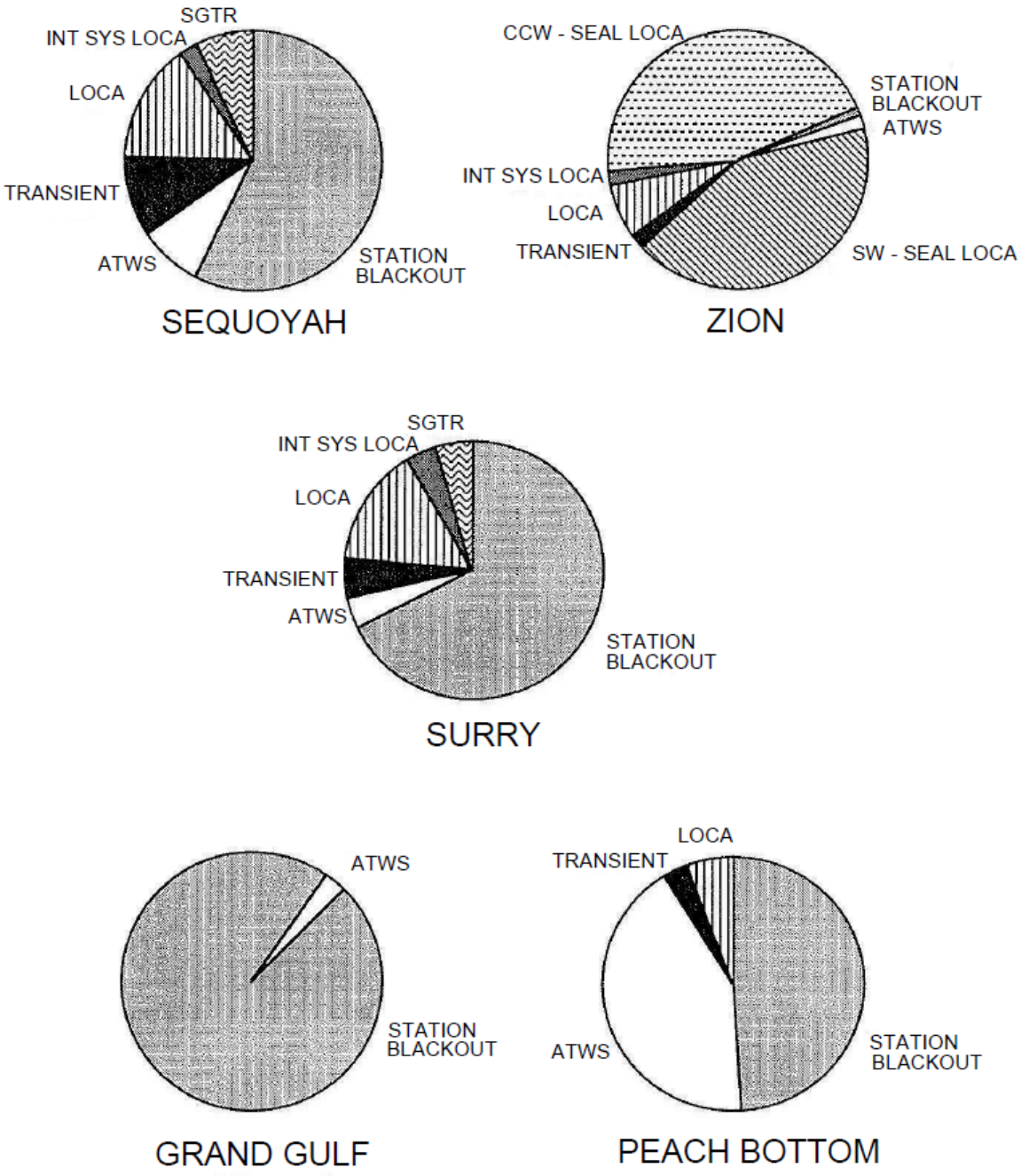


Figure 1.4-1 Major Contributors to Core Damage by Accident Types

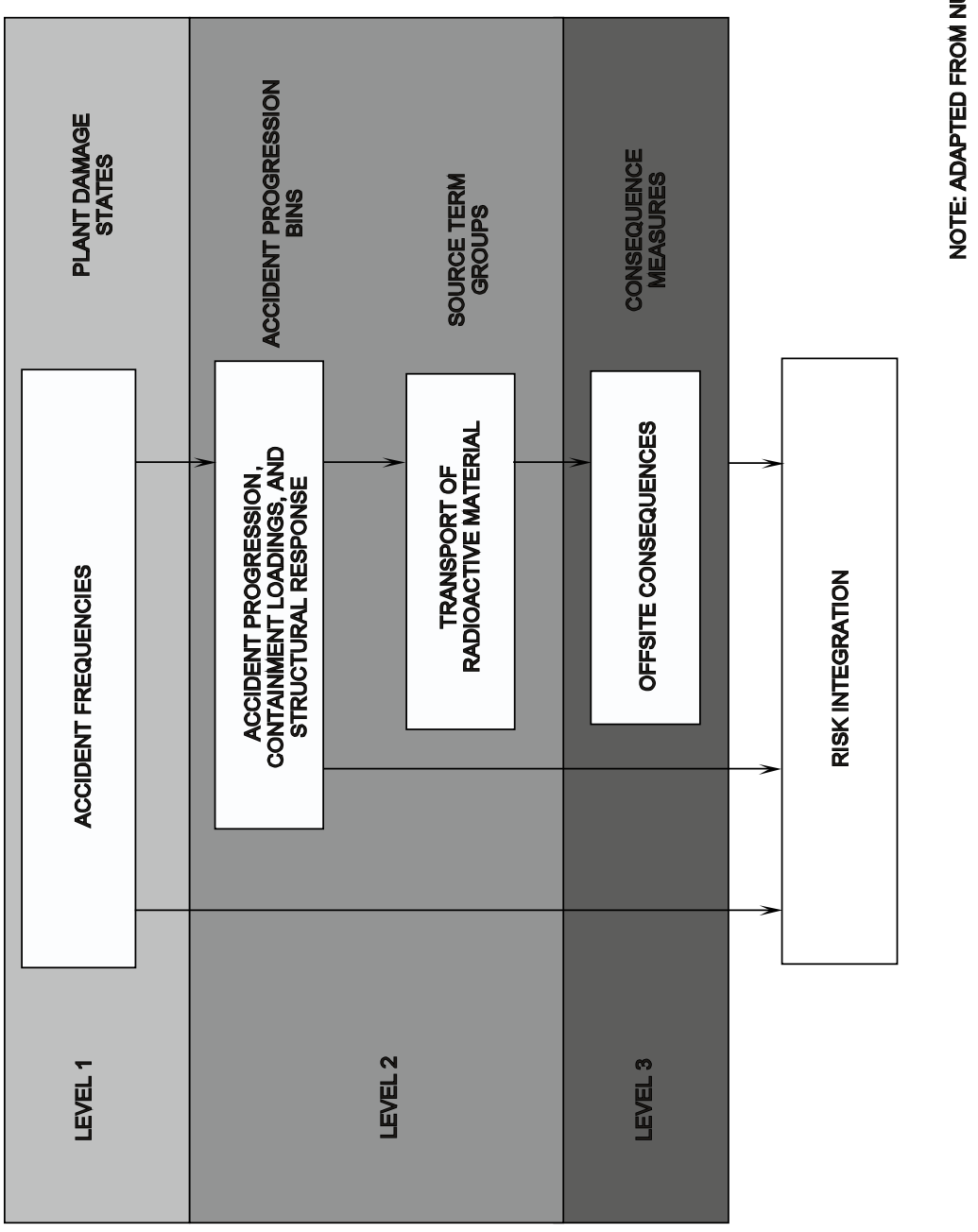


Figure 1.4-2 Principal Steps in Risk Anlaysis Process

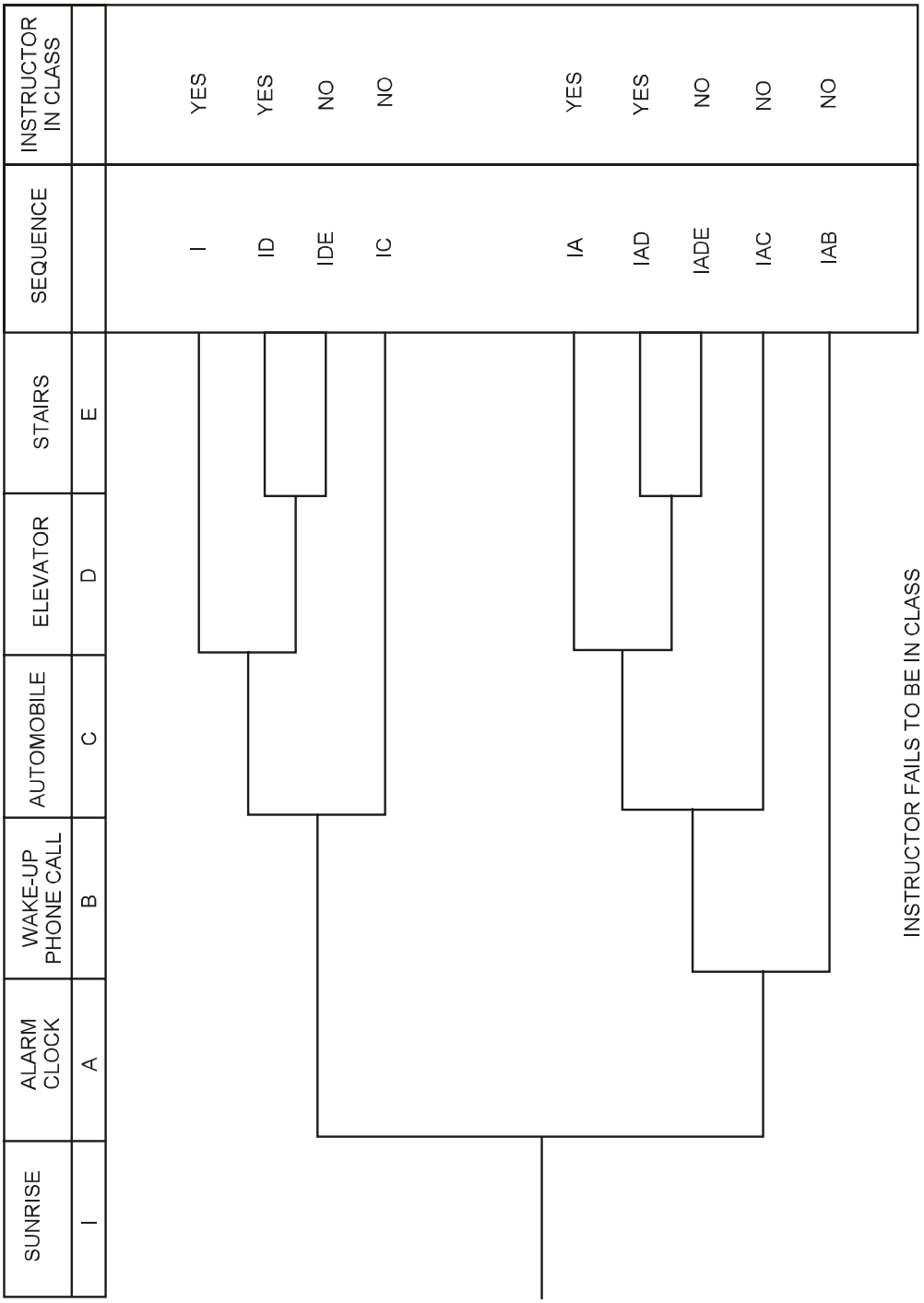


Figure 1.4-3 Event Tree Analysis

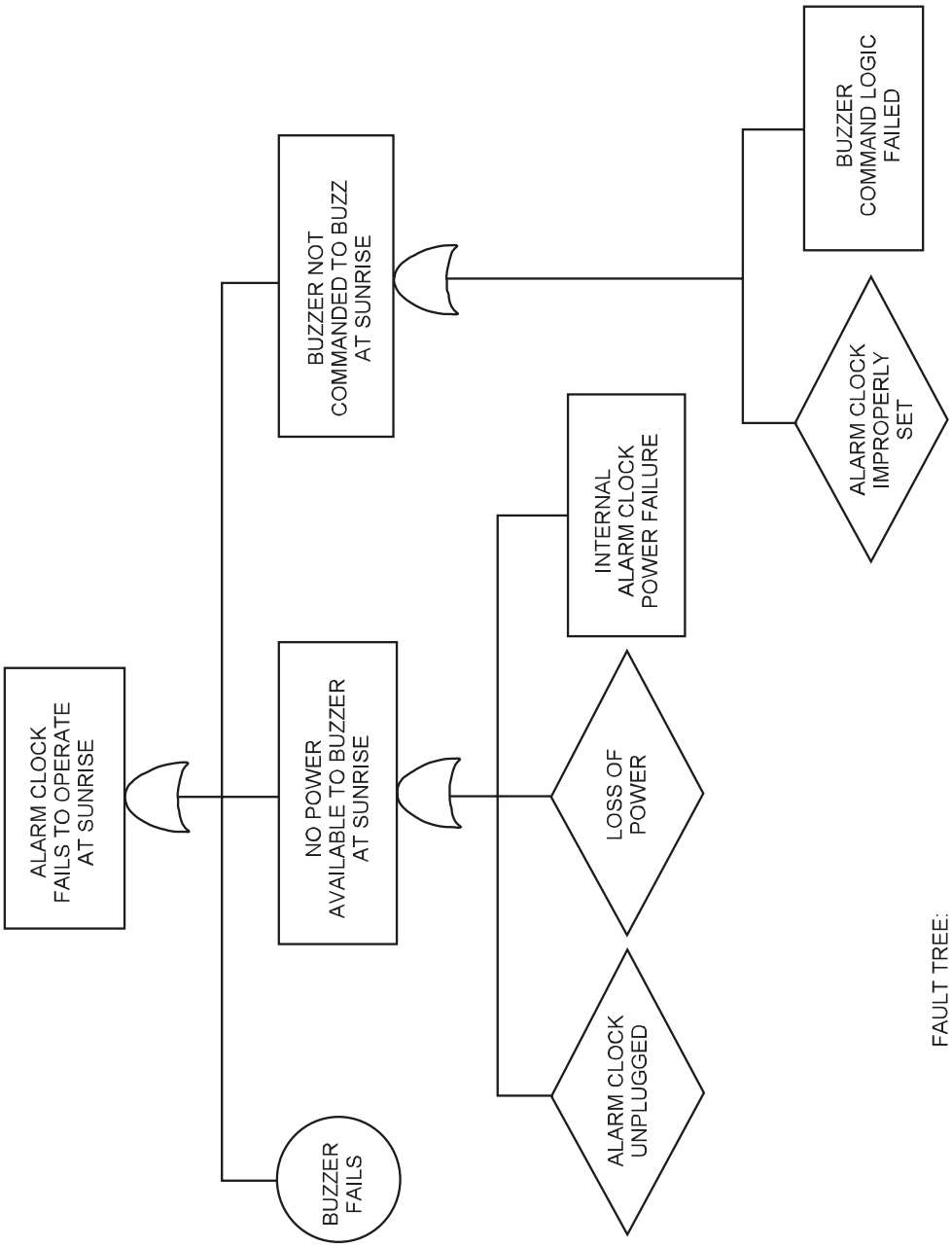


Figure 1.4-4 Fault Tree

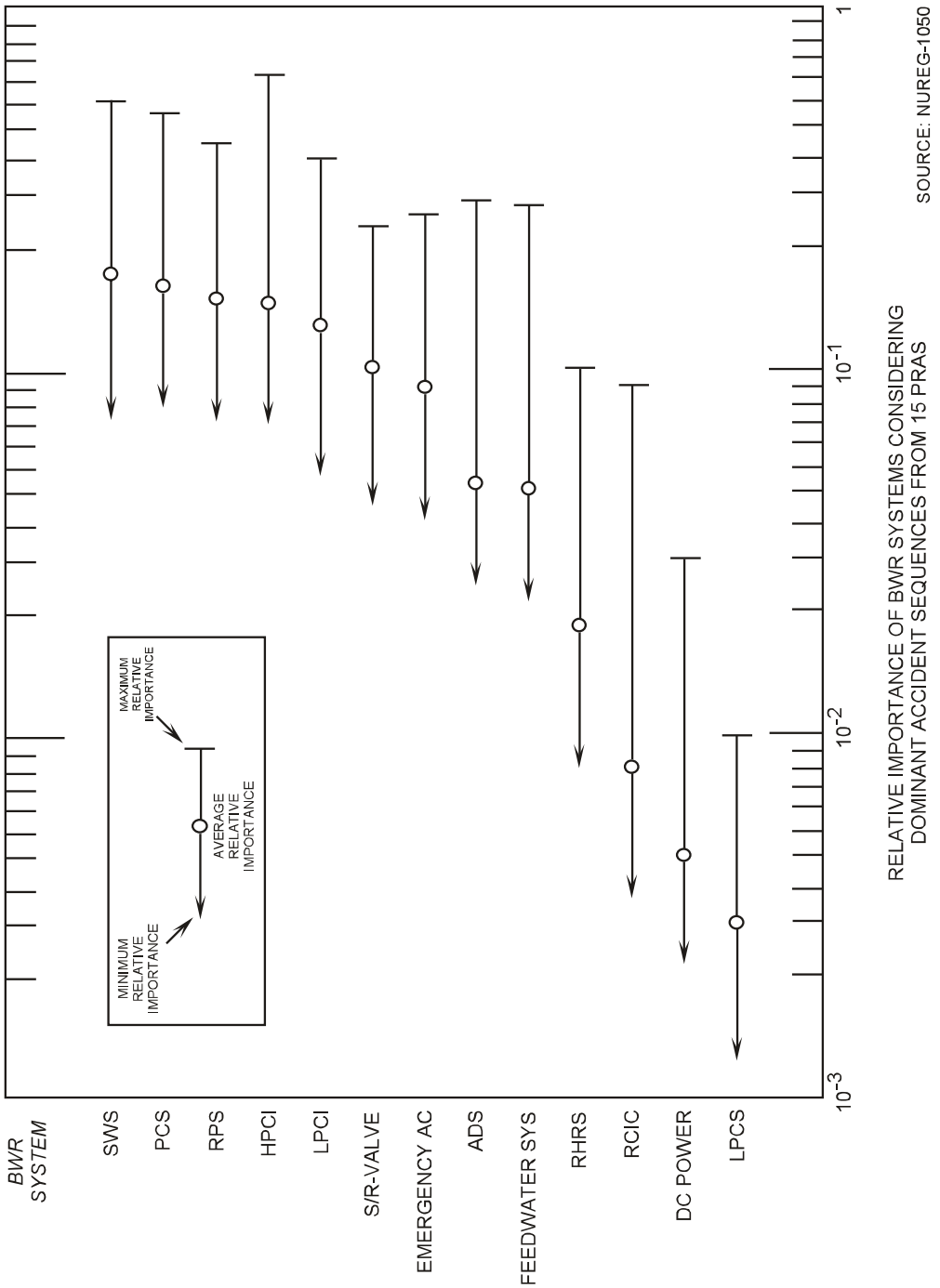


Figure 1.4-5 Relative Importance Factors

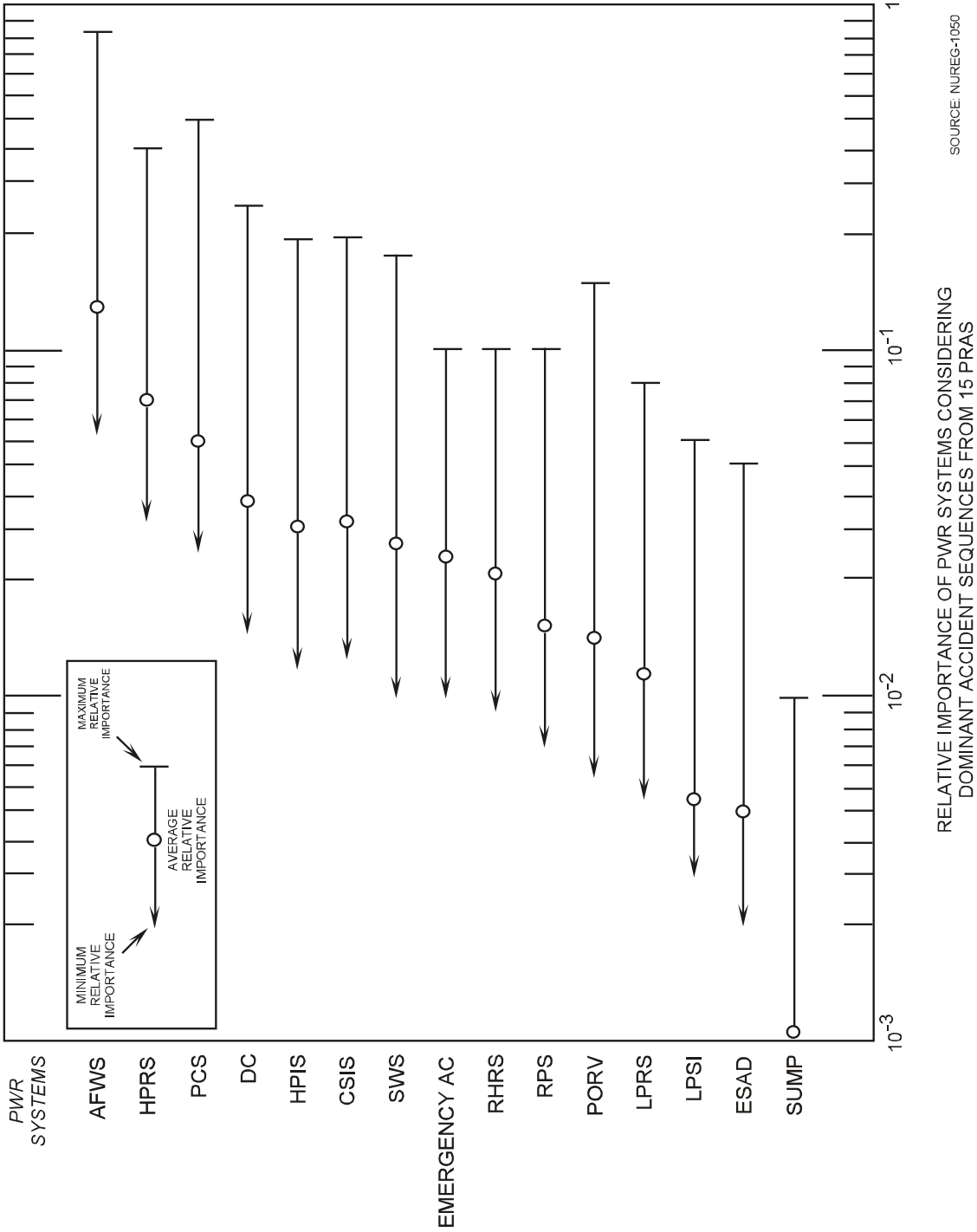
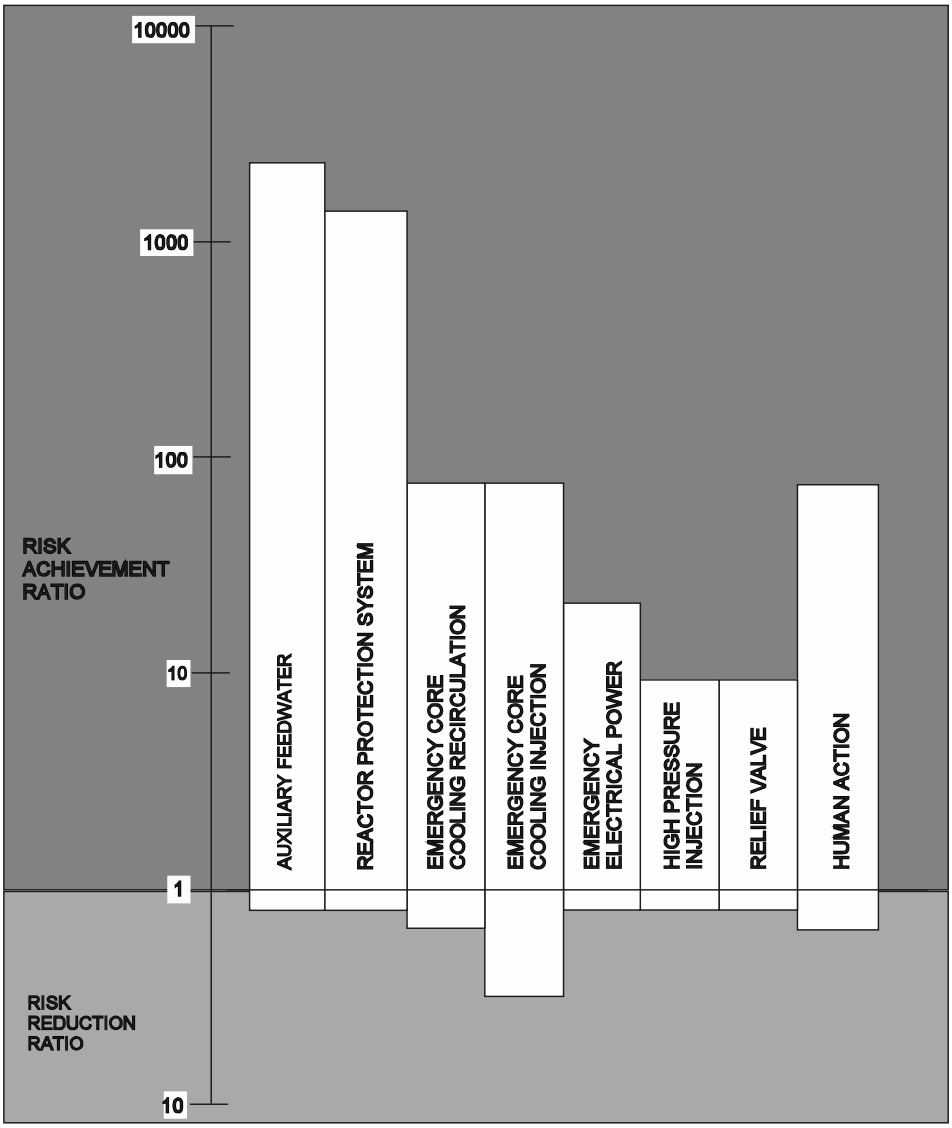


Figure 1.4-6 Relative Importance Factors



NOTE: RISK-WORTH RATIOS FOR SEQUOYAH SAFETY SYSTEMS WITH REGARD TO CORE-MELT FREQUENCY.
SOURCE: NUREG-1050

Figure 1.4-7 Risk-Worth Ratios