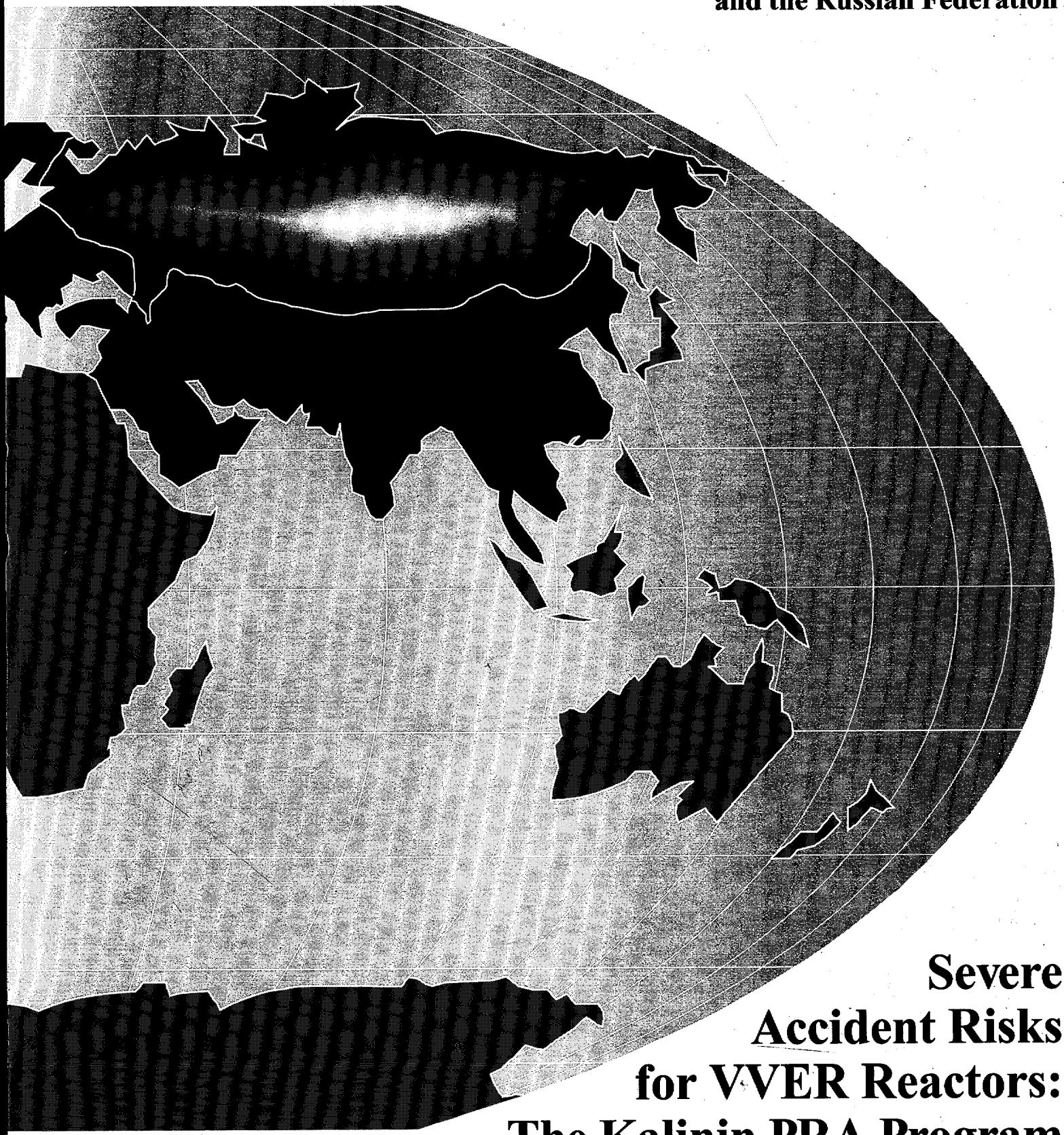
A Joint Cooperative Program Between
the Governments of the United States
and the Russian Federation



Severe Accident Risks for VVER Reactors: The Kalinin PRA Program

Volume 3: Procedure Guides

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy,* of the *Code of Federal Regulations,* may be purchased from one of the following sources:

1. The Superintendent of Documents
   U.S. Government Printing Office
   P.O. Box 37082
   Washington, DC 20402–9328
   <http://www.access.gpo.gov/su_docs>
   202–512–1800

2. The National Technical Information Service
   Springfield, VA 22161–0002
   <http://www.ntis.gov/ordernow>
   703–487–4650

The NUREG series comprises (1) brochures (NUREG/BR-XXXX), (2) proceedings of conferences (NUREG/CP-XXXX), (3) reports resulting from international agreements (NUREG/IA-XXXX), (4) technical and administrative reports and books [(NUREG-XXXX) or (NUREG/CR-XXXX)], and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Office Directors' decisions under Section 2.206 of NRC's regulations (NUREG-XXXX).

A single copy of each NRC draft report is available free, to the extent of supply, upon written request as follows:

Address: Office of the Chief Information Officer
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555–0001
E–mail: <DISTRIBUTION@nrc.gov>
Facsimile: 301–415–2289

A portion of NRC regulatory and technical information is available at NRC's World Wide Web site:

<http://www.nrc.gov>

All NRC documents released to the public are available for inspection or copying for a fee, in paper, microfiche, or, in some cases, diskette, from the Public Document Room (PDR):

NRC Public Document Room
2120 L Street, N.W., Lower Level
Washington, DC 20555–0001
<http://www.nrc.gov/NRC/PDR/pdr1.htm>
1–800–397–4209 or locally 202–634–3273

Microfiche of most NRC documents made publicly available since January 1981 may be found in the Local Public Document Rooms (LPDRs) located in the vicinity of nuclear power plants. The locations of the LPDRs may be obtained from the PDR (see previous paragraph) or through:

<http://www.nrc.gov/NRC/NUREGS/SR1350/V9/lpdr/html>

Publicly released documents include, to name a few, NUREG-series reports; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigation reports; licensee event reports; and Commission papers and their attachments.

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, Two White Flint North, 11545 Rockville Pike, Rockville, MD 20852–2738. These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
<http://www.ansi.org>
212–642–4900

NUREG/CR-6572, Vol. 3 Part 1
BNL-NUREG-52534

Severe Accident Risks for VVER Reactors: The Kalinin PRA Program

Volume 3: Procedure Guides

Manuscript Completed: May 1999
Date Published: September 1999

Brookhaven National Laboratory
Upton, NY 11973-5000

Prepared for
Division of Risk Analysis and Applications
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC Job Code R9608

ABSTRACT

In order to facilitate the probabilistic risk assessment (PRA) of a VVER-1000 nuclear power plant, a set of procedure guides has been written. These procedure guides, along with training supplied by experts and supplementary material from the literature, were used to advance the PRA carried out for the Kalinin Nuclear Power Station in the Russian Federation. Although written for a specific project, these guides have general applicability. For a Level 1 PRA (determination of core damage frequency for different scenarios), the guides are written for all of the technical tasks involved for internal events, including internal fires and floods and seismic events. Guides are also provided for a Level 2 PRA (probabilistic accident progression and source term analysis) and a Level 3 PRA (consequence analysis and integrated risk assessment). In addition, introductory material is provided to explain the rationale and approach for a PRA. Procedure guides are also provided on the quality assurance and documentation requirements.

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

Page

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

PART D - OTHER EVENTS - LEVEL 1 GUIDELINES

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

Page

TABLE OF CONTENTS
(Continued)

Page

PART 2 - APPENDICES (To Be Provided)

LIST OF FIGURES

LIST OF TABLES

FOREWORD

This is one of five volumes (see Figure 1) documenting the Probabilistic Risk Assessment (PRA) that was carried out for the Kalinin Nuclear Power Station (KNPS) in the Russian Federation (R.F.). The project was designed to improve reactor safety and regulation in the R.F. by building a framework to address reactor safety issues.

The project came about as a result of the Lisbon Conference on Assistance to the Nuclear Safety Initiative, held in May 1992, where it was agreed that special efforts should be undertaken to improve the safety of the nuclear power plants designed and built by the former Soviet Union. As part of these efforts, the U.S. Department of State,together with the Agency for International Development (AID),requested that the U.S. Nuclear Regulatory Commission (NRC) and the Federal Nuclear and Radiation Safety Authority of the Russian Federation (GAN) work together to begin the application of PRA technology to Soviet designed plants. As a result, the NRC and GAN agreed to work together to carry out a PRA of a VVER-1000 reactor in the R.F. NRC was to provide financial support for the PRA with funds from AID and technical support primarily through Brookhaven National Laboratory and its subcontractors. Unit 1 at the KNPS was chosen for the PRA, and the effort was carried out under the auspices of GAN with the assistance of five other Russian organizations:

- Science and Engineering Centre for Nuclear and Radiation Safety (GAN's semi-independent technical support organization)
- Kalinin Nuclear Power Station
- Experimental and Design Office "Gidropress" (the VVER designer)
- Nizhny Novgorod Project Institute "Atomenergoprojekt" (the architect-engineer)
- Rosenergoatom Consortium (the utility owner of KNPS).

The first volume documenting the PRA, "Kalinin Project Summary," contains the objectives of the project, a summary of how the project was carried out, and a general summary of the results of the PRA. The PRA considered only the reactor core as a potential source and only full power operation. A Level 1 PRA (assessment of core damage frequency) was carried out in detail along with a simplified Level 2 PRA (containment performance). This volume was written jointly by the Russian-American project team. The audience for this volume will be anyone interested in understanding what needs to be done to successfully complete such a project as well as the layperson who is interested in the results of the PRA.

The second volume, "Technical Summary of the Kalinin Probabilistic Risk Assessment," summarizes the frequency of finding the plant in some degraded state and the chance of damage, given that condition. It was written jointly by the Russian-American team for people with a technical background not necessarily expert in PRA. It provides the technical community with a perspective to understand the risk of nuclear operations if they are familiar with public risk from other sources. Event sequence diagrams and explanatory information are used to provide physical detail about the scenarios that are possible.

The third volume, "Procedure Guides for a Probabilistic Risk Assessment," documents the technical approach used for the PRA. It was written by the U.S. team and was made available at an early stage of the project in order to guide the work being done in the R.F. The guides helped to assure that the PRA would be done according to an internationally acceptable and consistent framework.

The fourth volume, "A Probabilistic Risk Assessment for the Kalinin Nuclear Power Station Unit 1 - Main Report," and the fifth volume, "A Probabilistic Risk Assessment for the Kalinin Nuclear Power Station Unit 1 - Appendices," were written by the Russians. The Main Report contains an explanation of the methods used and the results of the overall analysis as well as the analysis done for subtasks within the PRA. More details on the analysis are found in the Appendices.

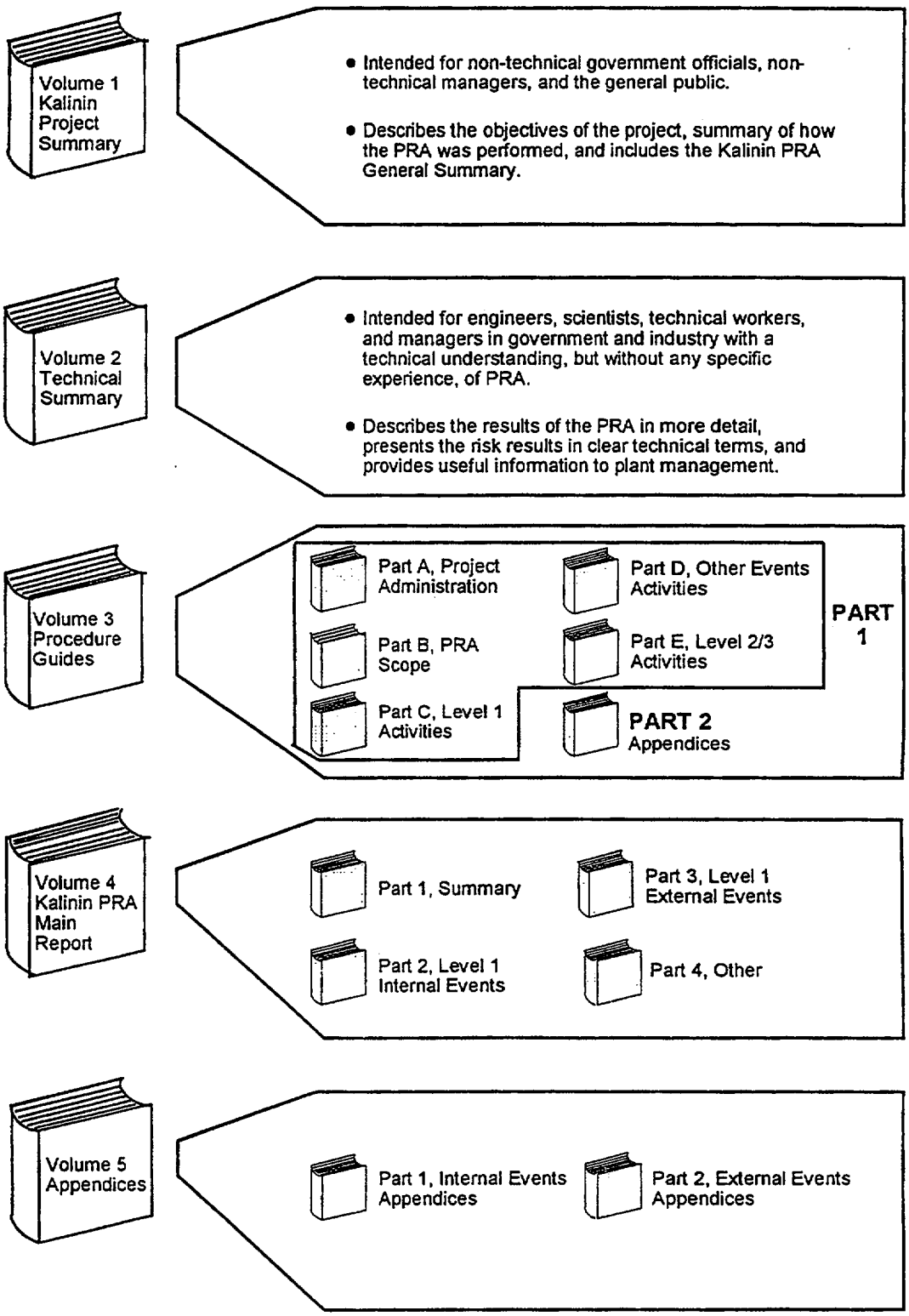


Figure 1 Documentation for the Kalinin PRA Project

ACKNOWLEDGMENTS

This activity was funded by the U.S. Agency for International Development.

Overall management and technical leadership of the project was provided by:

David Diamond (BNL)
Andrew Szukiewicz (NRC)
John Lane (NRC)
John Lehner (BNL)

The principal authors of this report were:

Dennis Bley (Buttonwood Consulting Inc.)
David Johnson (PLG Inc.)
Tsong-Lun Chu (BNL)
Mohamad A. Azarm (BNL)
Hossein Nourbakhsh (BNL)
Vinod Mubayi (BNL)
William T. Pratt (BNL)
Mary Drouin (NRC)

Other Contributors include:
Dr. Adel El-Bassioni (NRC)
John Flack (NRC)
Robert Youngblood (Scientech Inc.)
John Boccio (BNL)
Theo Theofanous (Univ. of Cal., Santa Barbara)
James Meyer (Scientech Inc.)

Editorial and Typing Support:
Cheryl Conrad (BNL)
Jean Frejka (BNL)
Patty Van Gurp (BNL)

ACRONYMS

ACRS	Advisory Committee on Reactor Safeguards
ANS	American Nuclear Society
AOIs	Abnormal Operating Instructions
BE	Basic Event
BNL	Brookhaven National Laboratory
CAR	Corrective Action Reports
CCF	Common-Cause Failure
CCI	Core-Concrete Interaction
CDF	Core Damage Frequency
CET	Containment Event Tree
DCH	Direct Containment Heating
DOE	U.S. Department of Energy
DRR	Document Review Records
EFC	Error-Forcing Context
EPRI	Electric Power Research Institute
ESD	Event Sequence Diagram
ET	Event Tree
FT	Fault Tree
F-V	Fussell-Vesely
GAN	Federal Nuclear and Radiation Safety Authority of the Russian Federation
HFE	Human Failure Event
HPI	High-Pressure Injection
HRA	Human Reliability Analysis
IAEA	International Atomic Energy Agency
IE	Initiating Event
INEL	Idaho National Engineering Laboratory
IMTS	Information Management and Tracking System
IRRAS	Integrated Reliability and Risk Analysis System
KNPS	Kalinin Nuclear Power Station
LOCA	Loss-of-Coolant Accident
MOV	Motor-Operated Valve
NRC	U.S. Nuclear Regulatory Commission

ACRONYMS
(Continued)

PCA	Probabilistic Consequence Assessment
PDS	Plant Damage State
PQASC	Project Quality Assurance Startup Checklists
PRA	Probabilistic Risk Assessment
PSF	Performance Shaping Factor
PWR	Pressurized Water Reactor
QA	Quality Assurance
QAR	Quality Assurance Audit Reports
QHO	Quantitative Health Objective
R.F.	Russian Federation
RAW	Risk Achievement Worth
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RRW	Risk Reduction Worth
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SLIM	Success Likelihood Index Method
SSC	Systems, Structures, and Components
SSMRP	Seismic Safety Margins Research Program
TRR	Technical Review Reports

PART 1

MAIN REPORT

1. INTRODUCTION

1.1 Background

At the Lisbon Conference on Assistance to the Nuclear Safety Initiative, held in May 1992, it was agreed that special efforts should be undertaken to improve the safety of the nuclear power plants designed and built by the former Soviet Union. As part of these efforts, the U.S. Department of State, together with the Agency for International Development (AID), requested that the U.S. Nuclear Regulatory Commission (NRC) and the Federal Nuclear and Radiation Safety Authority of the Russian Federation (GAN) work together to begin the application of PRA technology to Soviet designed plants. As a result, the NRC and GAN agreed to work together to carry out a probabilistic risk assessment (PRA) of a VVER-1000 reactor in the Russian Federation (R.F.).

Unit 1 at the Kalinin Nuclear Power Station (KNPS) was chosen for the PRA and the effort was carried out under the auspices of GAN with the assistance of several other Russian organizations.[1] The procedure guides in this document were written to advance the PRA which is intended to serve as a demonstration of the PRA process and its utility in the regulatory process and in plant operations. Furthermore, it is expected that the overall project will also advance the use of PRA methods and results in the regulation of nuclear power plants of VVER design not only in the R.F. but also in other countries with such reactors.

1.2 Objectives

In order to carry out the PRA for KNPS Unit 1, it was decided that the methodology for doing a PRA should be defined and explained in a set of guides. The writing of the guides would help assure that the PRA would be done according to an internationally acceptable and consistent framework. After individual tasks were completed the guides could then be used to help in the review of that work.

[1]In addition to GAN, the following organizations were involved: GAN's Scientific and Engineering Center for Nuclear and Radiation Safety, Kalinin Nuclear Power Station, the Experimental and Design Office Gidropress, Nizhny Novgorod Project Institute Atomenergoproect, and Rosenergoatom Consortium.

The first draft of the guides was used for the Kalinin PRA and now this final report should be useful to PRA practitioners in other countries, in particular those with VVER plants. For the Kalinin PRA these guides complemented other forms of technical assistance provided by the NRC--namely, classroom training and workshops. Therefore, it must be recognized that the guides alone will not provide the assistance needed to successfully complete a PRA for an organization that is relying on outside assistance.

1.3 Scope of the Procedure Guides

A PRA of a nuclear power plant is an analytical process that quantifies the potential risk (with regard to the health and safety of the public) associated with accident sequences that are functions of the design, operation, and maintenance of the plant. There are a number of major components that comprise a PRA as illustrated in Figure 1.1. The project administration component impacts all other aspects of the PRA and consists of establishing an appropriate quality assurance program, plant familiarization supported by an adequate information management scheme, and documentation of the results of the PRA.

The other components illustrated in Figure 1.1 define the scope of the PRA. It is necessary to identify all potential sources of radioactivity and decide on how many of these sources will be included in the PRA. It is also necessary to determine the spectrum of consequence measures to be considered (e.g., health effects to the plant personnel or the surrounding population). Accidents can occur while the plant is at full power, low power, or during a shutdown condition. The plant operating states to be considered in the PRA should, therefore, be clearly identified. The type of possible events that can initiate an accident also needs to be defined. Initiating events internal to the plant usually include transients, loss-of-coolant accidents (LOCAs), fires, and floods. Events external to the plant include seismic events, high wind, and others. Evaluation of sabotage events is not currently included in a full-scope PRA.

A complete PRA involves three sequential analytical parts or "levels" as shown in Figure 1.1:

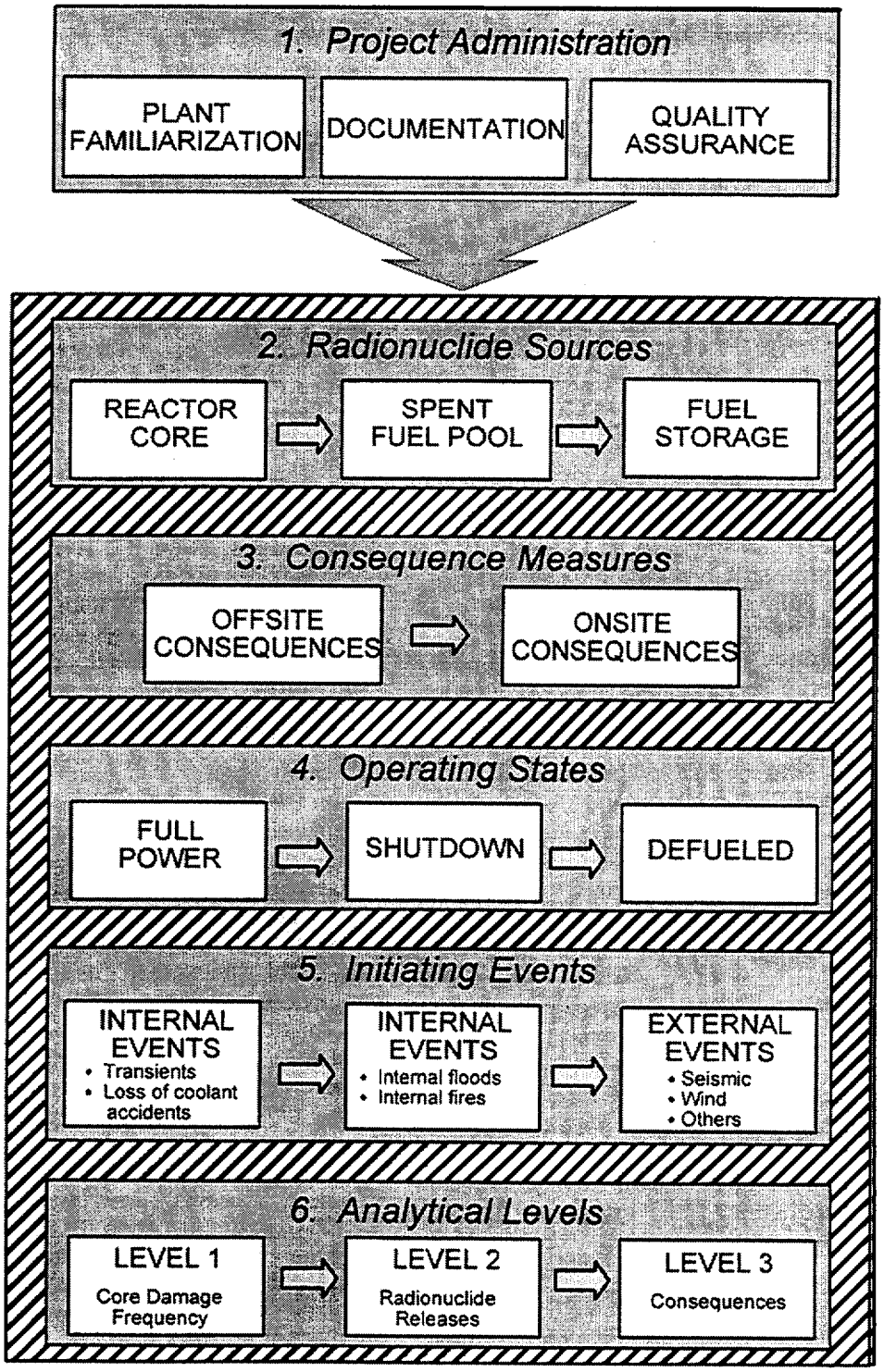


Figure 1.1 The six components comprising a PRA

- Level 1 - involves the identification and quantification of the sequences of events leading to core damage;
- Level 2 - involves the evaluation and quantification of the mechanisms, amounts, and probabilities of subsequent radioactive material releases from the containment; and
- Level 3 - involves the evaluation and quantification of the resulting consequences to both the public and the environment. Consequences to plant personnel are usually not included in a Level 3 PRA.

The procedure guides contained in this report do not cover all of the items discussed above and shown in Figure 1.1. The scope of the guidance in this report is illustrated in Figure 1.2. The guidance is limited to accidents involving only the reactor core and that occur while the plant is operating at full power. Initiating events internal and external to the plant are considered and included in the scope of this report. Guidance is also provided for all three analytical levels. However, the Level 3 PRA guidance is limited to offsite consequences.

1.4 Limitations and General Comments

It was assumed that the team carrying out the PRA would be familiar with the set of guides developed by the International Atomic Energy Agency (IAEA,1992) for carrying out a Level 1 PRA for internal events. The IAEA document represented an internationally acceptable approach. The new guides were to improve on the existing guides by: (1) taking into account recent work in the field, (2) considering special problems that might be specifically present for the VVER experience, and (3) improving upon the guidance already provided. The idea was not to duplicate the existing guidance found in the IAEA document or the material in other guides that have been produced by the NRC, e.g., NRC (1981) and Drouin (1987). For subjects not well documented in the open literature (e.g., the approach taken for human reliability analysis), detailed guidance would be given; for tasks where a firm understanding was already well established and documentation freely available (e.g., system modeling), minimal guidance and appropriate references would be provided.

Certain general assumptions and limitations are imposed on the scope and boundary conditions of a PRA. The following assumptions are usually found in a PRA:

- The plant is operating within its regulatory requirements.
- The design and construction of the plant are adequate and satisfy the established design criteria for the plant.
- Plant aging effects are not modeled; that is, constant equipment failure rates are assumed.

  A "freeze" date of the PRA is selected to represent the design, operation, and maintenance of the plant. To ensure that the PRA model is as current as possible at the end of the analysis and, therefore, represents (as practicable as possible) the as-built and as-operated plant, the design, operation, and maintenance of the plant as reflected at the beginning of the PRA analysis is selected as the freeze date.
- A minimum mission time of 24 hours is used in analyzing the accident sequences in a PRA; however, the mission time should be extended in a PRA when the core melt progression and potential releases have not yet been terminated and reactor pressure vessel and containment integrity are still challenged.
- The PRA is calculated for an "average" plant configuration. The plant can be in many different configurations (especially during shutdown) for short periods of time and it is not practical to calculate the risk from all of the potential configurations. Instead, the average plant risk is calculated using test and maintenance outage events in the PRA models to represent average unavailabilities of systems (or portions of systems). The

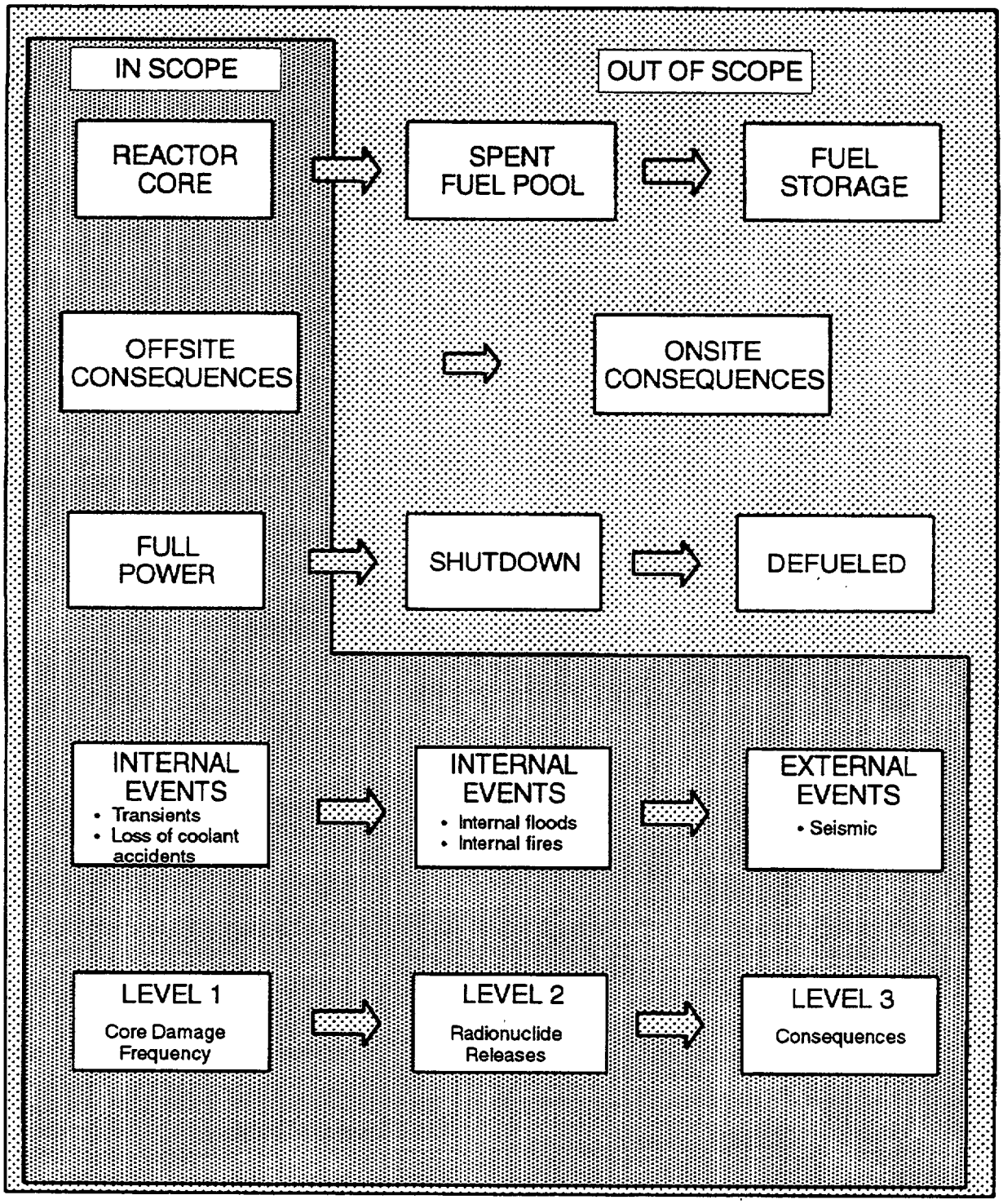


Figure 1.2 Scope of these procedure guides

average system unavailabilities reflect the availability of the systems during all the different configurations actually experienced in the past operation of the plant. The actual test and maintenance unavailabilities for the plant systems thus must be calculated using plant-specific operational data.

1.5 PRA Activities

The potential scope of a PRA is defined in the above sections. In this section, the general elements and specific analytical tasks needed to perform the PRA are briefly described. The tasks are described for each analytical level (i.e., Level 1, 2, or 3) covering accidents (involving the reactor core) caused by internal and external events while the plant is operating at full power.

1.5.1 Level 1 PRA

A Level 1 PRA comprises the following three major elements:

1. Identification and delineation of those sequences of events that, if not prevented, could result in a core damage state and the potential release of radionuclides,

2. Development of models that represent the core damage sequences,

3. Quantification of the models used in estimating the core damage frequency.

Figure 1.3 illustrates the relationships between the "analytical" activities associated with each of the above elements (discussed below).

1.5.1.1 Identification and Delineation of Accident Sequences (Element 1)

The first element of a Level 1 PRA identifies and delineates those sequences of events that, if not prevented, could result in a core damage state and a potential release of radionuclides. This process typically involves identification of the initiating events and development of the potential core damage accident sequences associated with the initiating events.

The identification of initiating events focuses on events that challenge normal plant operation and require successful mitigation in order to prevent core damage. Since there can be tens or hundreds of such events, this task also includes grouping the individual events into initiating event classes within which all events have similar characteristics and require the same overall plant response.

Accident sequence analysis involves identifying and delineating the different possible sequences of events that can evolve as a result of each initiating event class. The resulting sequences depict the different possible combinations of functional and/or system successes and failures (and operator actions) that lead either to successful mitigation of the initiating event or to the onset of core damage. Determination of what constitutes success (i.e., success criteria) to avert the onset of core damage is a crucial part of the accident sequence development task.

1.5.1.2 Systems Analysis (Element 2)

The second element of a Level 1 PRA involves the development of models for the mitigating systems and for actions delineated in the core damage accident sequences. This process typically is mostly a single task referred to as "systems modeling." This task involves modeling the failure modes of the plant systems that are necessary to prevent core damage (as defined by the core damage accident sequences). This modeling process, involving the use of fault trees, defines the combinations of equipment failures, equipment outages (such as for test or maintenance), and human errors that cause failure of the systems to perform the desired functions. Another important task is to identify any spatial interactions that need to be reflected in the systems analysis. It is also necessary to ensure that any dependences and interfaces between and among the systems and components are included in the model.

1.5.1.3 Quantification (Element 3)

The third element of a Level 1 PRA involves the quantification of the plant's core damage frequency and the associated statistical uncertainty. This process typically involves several tasks within data analysis, human

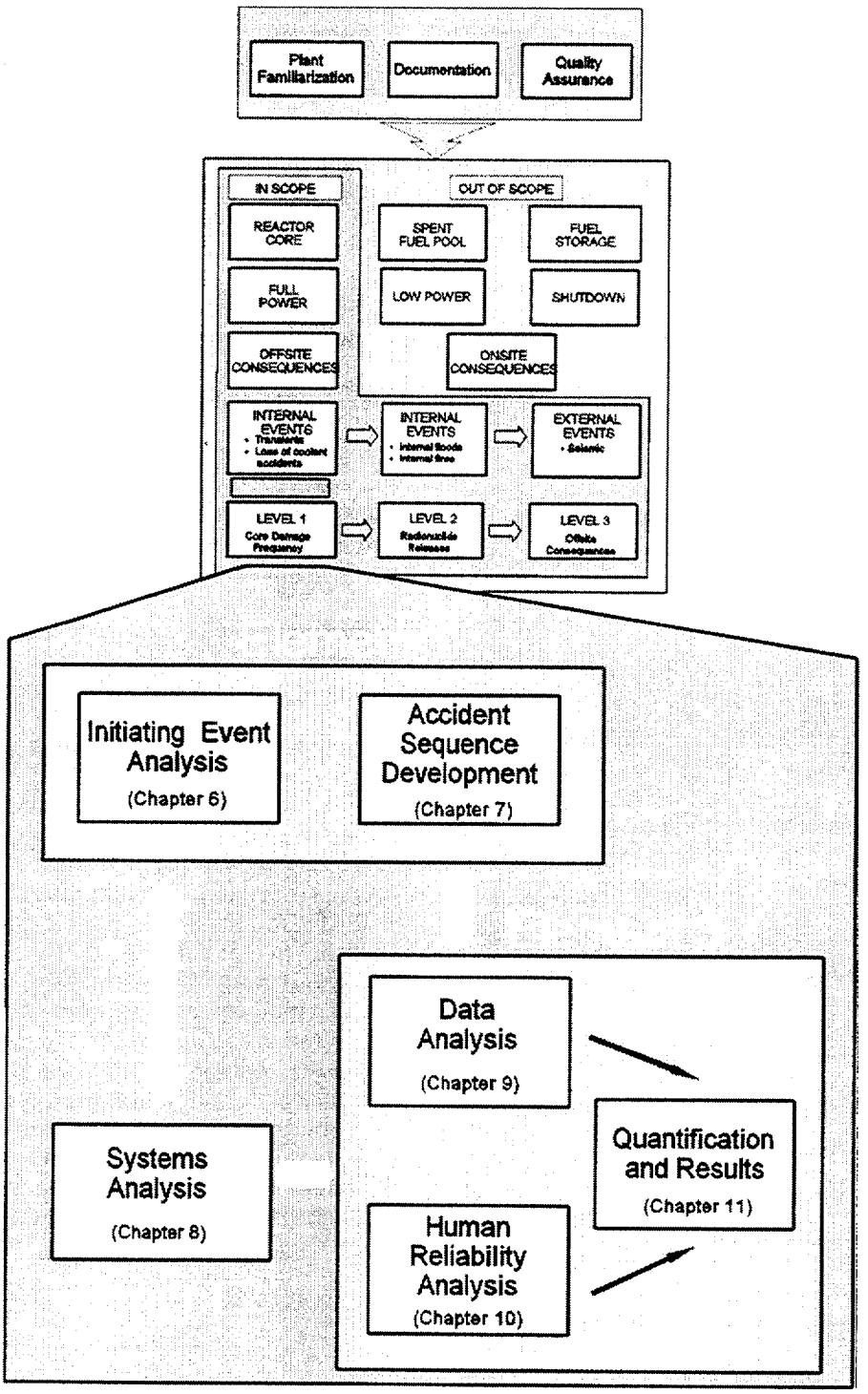


Figure 1.3 Analytical activities for a Level 1 internal event PRA

reliability analysis, and quantification and uncertainty analysis.

The data analysis involves tasks for determining initiating event frequencies, equipment failure probabilities (including common-cause failure probabilities), and equipment maintenance unavailabilities. Plant maintenance and other operating records are evaluated to derive plant-specific equipment failure rates and the frequencies of the initiating events.

The human reliability analysis task involves evaluating the human actions that are important to prevent and mitigate core damage. This evaluation involves identifying the operator actions and quantifying the error probabilities of these actions. Human reliability analysis is a special area of analysis requiring unique skills to determine the types and likelihoods of human errors germane to the sequences of events that could result in core damage and radionuclide releases.

The quantification and uncertainty analysis involves integrating the initiating event frequencies, event probabilities, and human error probabilities into the accident sequence models in order to calculate the average annual core damage frequency and its associated uncertainty. The uncertainty analysis reflects the lack of precision in the data or a lack of detailed understanding of the modeled phenomena. The sensitivity of the model results to model boundary conditions and other key assumptions can be evaluated using sensitivity analyses to look at key assumptions or parameters both individually and in logical combinations. In addition, importance measure calculations can be performed to provide information regarding the contributions of various components and basic events to the model estimation of the total core damage frequency.

1.5.2 Level 1 PRA - Other Events

The analytical activities associated with a Level 1 PRA for sequences initiated by events internal to the plant (such as transients and LOCAs) are described in the previous section. Other events both internal and external to the plant can cause unique initiating events or influence the way in which a plant responds to an accident. Figure 1.4 identifies three types of events (i.e., internal fires, internal floods, and seismic events) that require manipulation of the Level 1 internal event PRA in order to adequately model the plant response. Level 1 PRAs for these events utilize the same overall analysis approach and procedures developed for the internal event PRA (Section 1.5.1). Differences in the PRAs for these type of events relate to identifying unique initiating events and the ways in which the plant response could be significantly affected by the event itself (such as multiple failures of redundant safety systems caused by a seismic event).

1.5.2.1 Internal Fire Analysis

There are many points of commonality between the internal events analysis and an internal fire analysis. These include the use of the same fundamental plant systems models (event trees and fault trees), similar treatment for random failures and equipment unavailability factors, similar methods of overall risk and uncertainty quantification, and similar methods for the plant recovery and human reliability analysis. Consistency of treatment of these commonalities is an important feature in an internal fire analysis. It is also important that documentation for an internal fire analysis parallel that for an internal events PRA, with supplemental documentation of any unique fire-related aspects of the analysis provided as necessary.

Although the overall evaluation process is the same, there are differences in the events postulated to occur in response to an internal fire. Differences arise from the fact that the fire analysis has to account for the effects of the fire and should provide for the specific treatment of the actual fire phenomena associated with the postulated fire event.

1.5.2.2 Internal Flood Analysis

A PRA covering an analysis of internal floods uses much of the same processes provided under the discussion of full power internal events (Section 1.5.1). However, an internal flood analysis requires significant work to define and screen the most important flood sources and possible scenarios for further evaluation. This requires consideration of different plant design features with particular emphasis on the spatial aspects of the plant's design. Consideration of structures, barriers, drainage designs, and

different failure modes (e.g., water submersion of equipment and water spray on electrical equipment) are examples of aspects of the plant that are considered in the internal flood analysis that are not necessarily addressed in the internal events analysis. After the flood scenarios have been screened for detailed quantification, the remaining work follows much of the same modeling and quantification already carried out in the internal events analysis with relatively minor modification.

1.5.2.3 Seismic Analysis

The objective of a seismic PRA is to analyze the risk due to core damage accidents initiated by earthquakes. This means that the frequency and severity of earthquakes should be coupled to models of the capacity of plant structures and components to survive each possible earthquake. The effects of structural failure should be assessed, and all the resulting information about the likelihood of equipment failure should be evaluated using the internal events PRA logic model of the plant modified as appropriate to include seismic-induced events.

The basic parts of a seismic PRA include (1) hazard analysis, (2) structure response analysis, (3) evaluation of component fragilities and failure modes, (4) plant system and sequence analysis, and (5) containment and containment systems analysis. One important aspect of a seismic event is that all parts of the plant are excited at the same time. This means that there may be significant correlation between component failures, and hence, the redundancy of safety systems could be compromised. The correlation could be introduced by common location, orientation, and/or vibration frequency. This type of "common-cause" failure represents a unique risk to the plant that must be reflected in a seismic PRA.

1.5.3 Level 2 PRA

A Level 1 PRA (described in Sections 1.5.1 and 1.5.2) provides information on the accident sequences that can lead to core damage and their associated frequency. As shown in Figure 1.5, this information is used as input to a Level 2 PRA. The primary objective of the Level 2 portion of a PRA is to characterize the potential for, and magnitude of, a release of radioactive material from the reactor fuel to the environment, given the occurrence of an accident sequence that damages the reactor core. To satisfy this objective, a Level 2 PRA is comprised of two major parts:

1. A structured and comprehensive evaluation of accident progression and containment performance in response to the accident sequence identified from the Level 1 analysis.

2. A quantitative characterization of radiological release to the environment that would result from accident sequences that involve bypass or failure of the containment pressure boundary.

A concern associated with the results of Level 2 PRAs stems from their known susceptibility to phenomenological uncertainties. These uncertainties are often of such a magnitude that they make the decision-making process difficult. There is much to be gained, therefore, from assessment of severe accident risks, by reformulation of the Level 2 methodology into a simplified containment event tree and redefinition of the phenomenological portion in terms of a physically based probabilistic framework. Such an approach provides a streamlined procedure for assessment of severe accident risks that allows for a direct evaluation of potential accident management strategies. This is the approach adopted in this report. Guidelines for a more detailed Level 2 PRA have been developed by the International Atomic Energy Agency (IAEA, 1995). In addition, the NRC has recently published NUREG-1560 (NRC, 1996), which contains a description of the characteristics of a state-of-the-art Level 2 PRA.

In addition to estimating the probability of a radiological release to the environment, the Level 2 portion of a PRA of a nuclear reactor characterizes the resulting release in terms of magnitude, timing, and other attributes important to an assessment of offsite accident consequences. This information has two purposes. First, it provides a quantitative scale for ranking the relative severity of various accident sequences; secondly, it represents the "source term" for a quantitative evaluation of offsite consequences (i.e., health effects, property damage, etc.), which are estimated in the Level 3 portion of a PRA (as indicated in Figure 1.5).

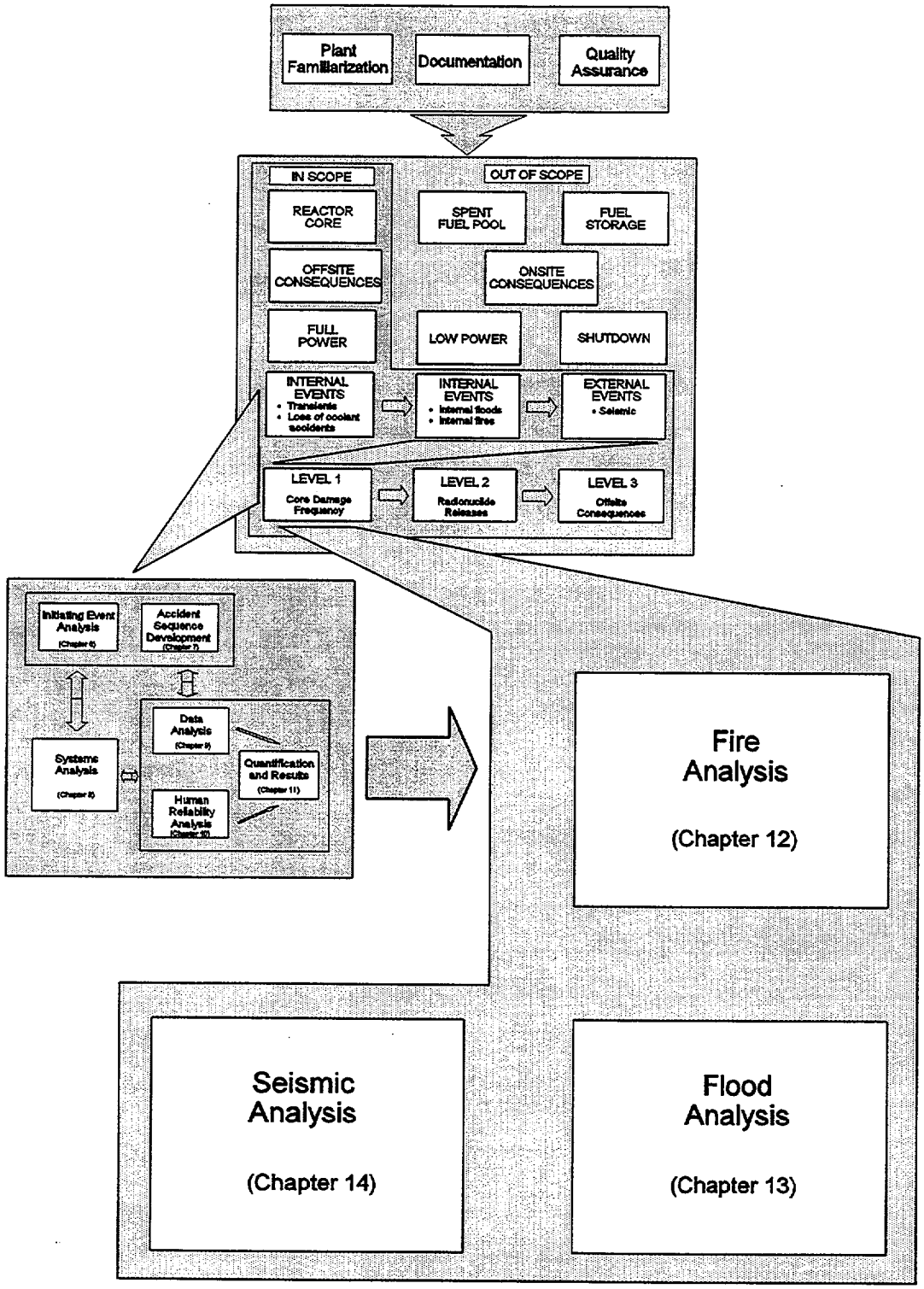


Figure 1.4 Other events that can influence a Level 1 PRA

1.5.4 Level 3 PRA

Analyses performed as part of the Level 3 portion of a PRA consist of two major parts:

1. Accident consequence analysis and
2. Computation of risk by integrating the results of Level 1, 2, and 3 analyses.

1.5.4.1 Accident Consequence Analysis

The offsite consequences of an accidental release of radioactive material from a nuclear power plant can be expressed in several forms including impacts on human health, the environment, or economics. The consequence measures of interest to a Level 3 PRA for a nuclear power plant focus on impacts on human health. These impacts are estimated both in societal terms and in terms of the most-exposed individual.

There are a number of computer codes that are currently in use that incorporate current, state-of-the-art models for estimating the consequences of postulated radiological releases. Performing consequence calculations requires a substantial amount of supporting information. Atmospheric dispersion models require the specification of local meteorology and terrain; deposition models require information regarding frequency and intensity of precipitation; dose and health effects models require information regarding local demographics and land use (i.e., crops grown, dairy activity). In an evaluation of accident consequences, this information represents current, site-specific conditions. It is not necessary to directly quantify and incorporate uncertainties in models for atmospheric dispersion, deposition, and health effects in the calculations of accident consequences. Although these uncertainties are generally acknowledged to be substantial, they are not currently included in Level 3 PRAs.

1.5.4.2 Computation of Risk

The final step in a Level 3 PRA is the integration of results from all previous analyses in order to compute individual measures of risk. The severe accident progression and the radionuclide source term analyses conducted in the Level 2 portion of the PRA, as well as the consequence analysis conducted in the Level 3 portion of the PRA, are performed on a conditional basis. That is, the evaluations of alternative severe accident progressions, resulting source terms, and consequences are performed without regard to the absolute or relative frequency of the postulated accidents. The final computation of risk is the process by which each of these portions of the accident analysis are linked together in a self-consistent and statistically rigorous manner.

1.6 Organization of this Volume

This volume is organized in two parts as shown in Figure 1.6. Part 1 provides the main guidance and Part 2 provides the appendices. Part 1 is divided into five "sub -parts" (A through E). Part A provides guidance for important aspects of project administration for a PRA and is divided into three chapters. Chapter 2 describes the important plant familiarization task and includes guidance on information gathering and establishing an information management system. Documentation requirements for all elements of the PRA are described in Chapter 3. Guidelines are provided in Chapter 4 on an appropriate approach for quality assurance for the PRA.

The PRA scope is discussed in Part B which consists of Chapter 5. The discussion includes consideration of the sources of radioactivity at the plant and the plant operating conditions.

Guidance for a Level 1 PRA is presented for different initiating events in Parts C and D. Part C includes guidance for each of the analytical tasks associated with internal events. This part of the report comprises the bulk of the guidance and is divided into six chapters. Chapter 6 provides guidance for identifying initiating events internal to the plant and is closely related to Chapter 7, which describes accident sequence development. Chapter 7 includes subsections that deal with the definition of core damage states, functional analysis and system success criteria, and event sequence modeling. The systems analysis is presented in Chapter 8. The systems analysis chapter includes guidance on system modeling, qualitative dependency analysis, and the assessment of spatial interactions. Chapter 9 describes the data analysis which includes assessments of initiating event frequencies, component reliability, and common-cause failure probabilities.

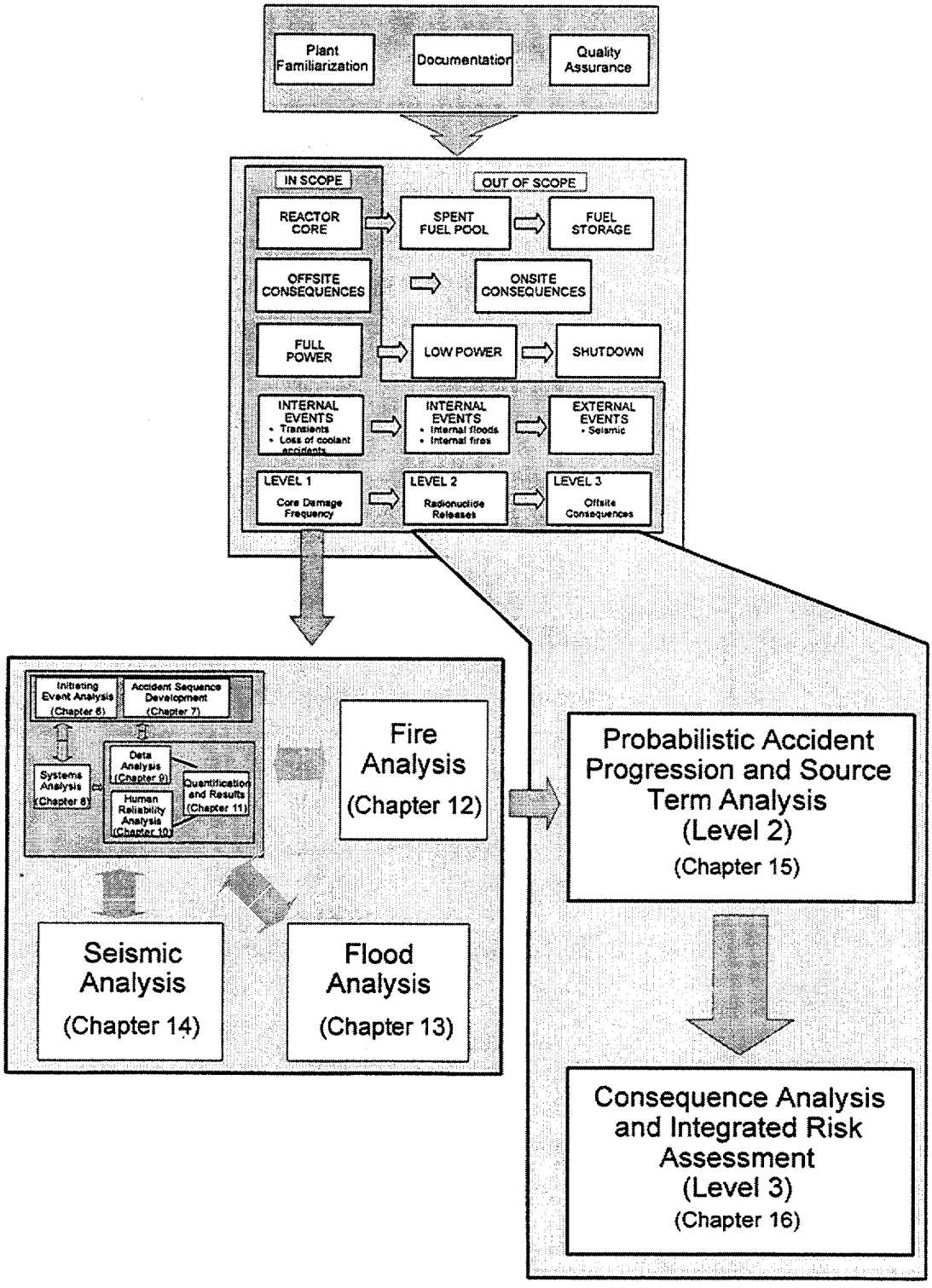


Figure 1.5 Elements of a Level 2 and Level 3 PRA

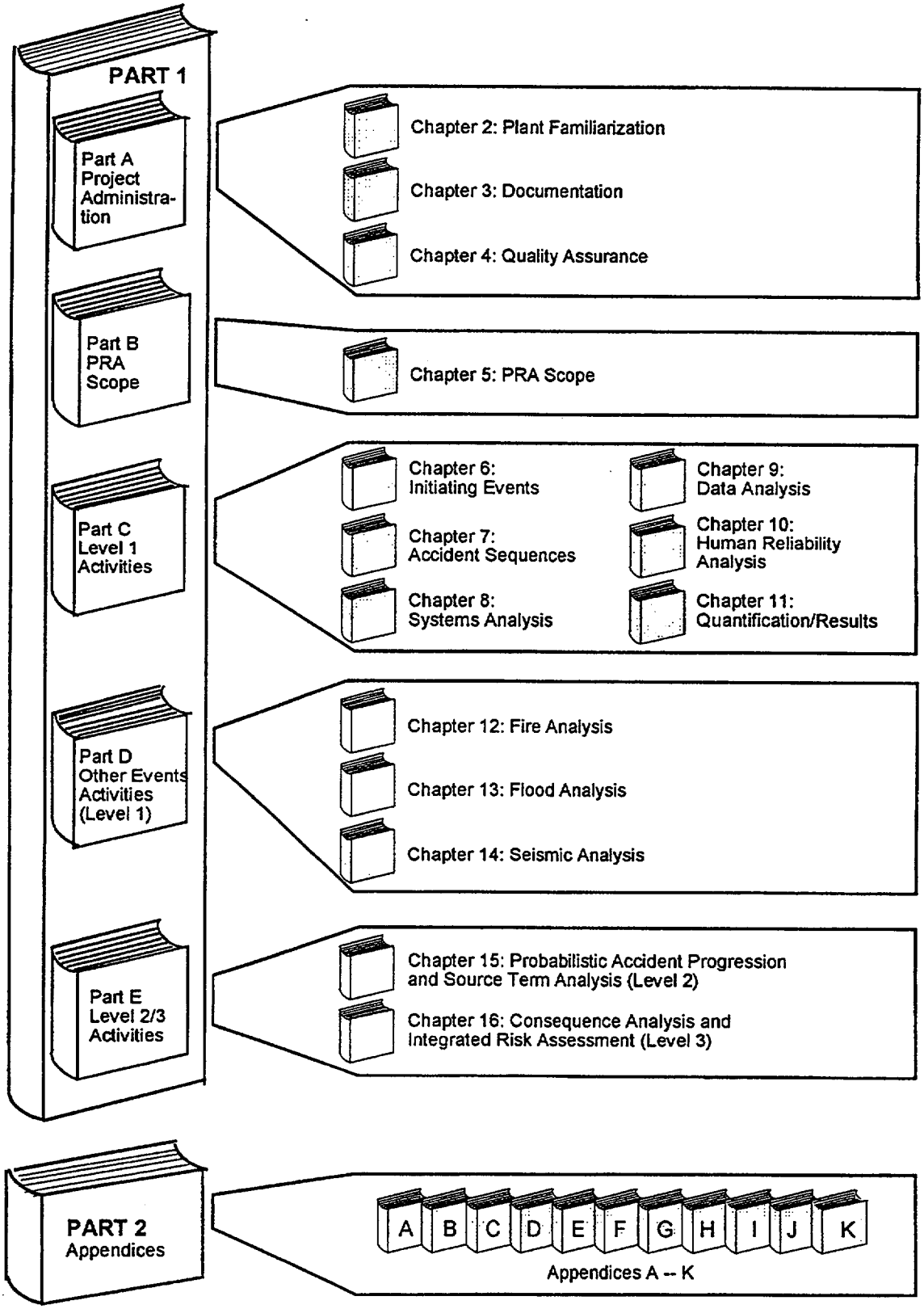


Figure 1.6 Organization of this volume

The human reliability analysis is described in Chapter 10. The final chapter in Part C deals with quantification, which includes initial and final quantification of the accident sequences, and sensitivity and importance analyses.

Part D is divided into three chapters. Chapter 12 describes how a Level 1 PRA would be developed to model fires internal to a plant. Considerations for constructing a Level 1 PRA for internal flooding is provided in Chapter 13. The attributes of a seismic analysis are presented in Chapter 14.

Part E addresses the analytical tasks associated with a Level 2 and Level 3 PRA. Chapter 15 provides guidance for performing an assessment of containment performance during severe accidents and on calculating the magnitude and likelihood of radionuclide release to the environment. Chapter 16 deals with an assessment of offsite consequences and consists of guidance for calculating offsite health effects and for integrating the Level 1, 2, and 3 analyses into an estimate of risk.

Lastly, all of the appendices to the report are included in Part 2.

1.7 References

Drouin, M. T., F. T. Harper, and A. L. Camp, "Analysis of Core Damage Frequency from Internal Events: Methodology, Volume 1," NUREG/CR-4550/1, Sandia National Laboratories, September 1987.

IAEA, "Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2)," Safety Series No. 50-P-8, International Atomic Energy Agency, 1995.

IAEA, "Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1)," Safety Series No. 50-P-4, International Atomic Energy Agency, 1992.

NRC, "Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance," NUREG-1560, U.S. Nuclear Regulatory Commission, 1996.

NRC, "PRA Procedures Guide - A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, U.S. Nuclear Regulatory Commission, September 1981.

PART A - PROJECT ADMINISTRATION

2. PLANT FAMILIARIZATION

The objectives of this task are to define and obtain the types of information necessary for performing the major analytical tasks of a probabilistic risk assessment (PRA). The Plant Familiarization task is an important activity associated with the project administration component of a PRA (refer to Figure 1.1). Figure 2.1 shows the important relationships between this task and the other major tasks of the PRA. These relationships are discussed below in Section 2.1.

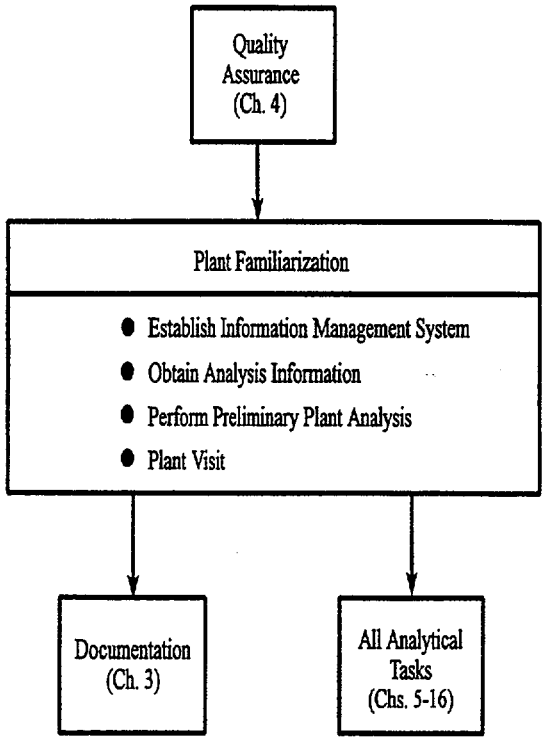


Figure 2.1 Relationships between plant familiarization and other tasks

2.1 Relation to Other Tasks

As identified in Figure 2.1, the current task provides significant information to all analytical tasks of the PRA. In addition, the task provides basic information needed for the final documentation. The figure also indicates the importance of applying the principles of quality assurance (QA) in this task and all other task activities. Guidelines for developing a QA program are described in Chapter 4.

2.2 Task Activities

An information management and tracking system (IMTS) will be developed and maintained throughout the life of the PRA. The IMTS will include a database of the documents and a document distribution log methodology consistent with the guidelines provided in the project's QA program. This database will help to keep track of the vast amount of plant information obtained and to ensure that the latest and most appropriate information is used consistently throughout the various analytical tasks. The IMTS should help to facilitate the timely distribution of current plant information to project team members. It should also establish an organizational structure showing lines of responsibility for the maintenance of a project information filing and data retrieving system.

After the additional information is obtained during the plant visit, the outputs of the preliminary plant analysis task (as described in Section 2.2.2.3) should be finalized to the extent possible before being employed in subsequent tasks in the PRA.

To complete this task successfully, the team should become thoroughly familiar with the design and operation of the plant, including items such as emergency procedures and test and maintenance procedures. Another objective of this task is to provide the team with a balanced overview of the basic issues in carrying out a PRA. Team members will acquire, according to their expertise and assigned area, in-depth knowledge of PRA methods and the plant, along with the necessary documentation and other information needed for specific task activities. Development of a system for updating and keeping track of the acquired documentation is also considered as part of this task. The quality of information gathered and the manner in which it is managed is critical to the success of the entire analysis effort. This information gathering process provides some assurance that the possible core damage accident sequences are correctly defined and that the possible plant responses are realistically described.

2.2.1 Assumptions and Limitations

This task provides the basic plant information needed to perform the analytical work. Hence,

the accuracy of the information gathered is crucial. If inaccurate information is used (e.g., a plant drawing that is out of date because a pump has been removed from the system without the drawing being updated), the final results are likely to inaccurately reflect the operational risk of the plant. It is, therefore, important that all information be verified, and a method for verifying plant information should be developed early in the project.

Verification is particularly important for VVER reactors because the information can come from several different sources. The team leader should establish an appropriate QA process so that the information does provide an accurate representation of the as-built condition and current operation of the plant. Note that this verification is also part of an overall QA program for the project.

The verification is aided by well organized and planned plant visits which in part look at the actual plant components and layout and compares them with written descriptions and diagrams. The verification is also aided by the establishment of a plant information data management and retrieval system which is described below.

The plant may not be a fixed entity. During (and after) the period of the PRA analysis, design and operational changes can occur at the plant. Many may not have a risk or safety impact. However, some of the changes could have the potential to significantly affect the final results of the analysis. At the start of the project, the team leader should decide on a configuration freeze date, i.e., the date after which plant changes will not be included in the analysis. Therefore, close communication must exist between the team leader and the plant staff member responsible for scheduling plant changes. This close coordination ensures that the analysts are not dealing with a moving target in terms of plant configuration. The potential for the analysis to be outdated before completion is reduced.

Establishing an analysis freeze date is intended to facilitate the completion of the models in a timely manner. Indeed, it is likely and desirable for plant changes (hardware or procedural) to be identified during the conduct of the PRA, possibly as a result of some preliminary task-analysis findings. If a commitment is made to implement these changes in a timely manner, the PRA should then incorporate them into the plant model after concurrence between the team leader and the project sponsors. It should be noted, however, that in a typical plant, changes ranging from small to major occur frequently. Consideration of all would be a major distraction of the project team and can impact project milestones.

2.2.2 Plant Familiarization Process

In this task, an understanding of the plant is established, providing the foundation for all subsequent technical analyses and modeling activities. This process involves several activities illustrated in Figure 2.2, summarized below, and subsequently discussed in more detail.

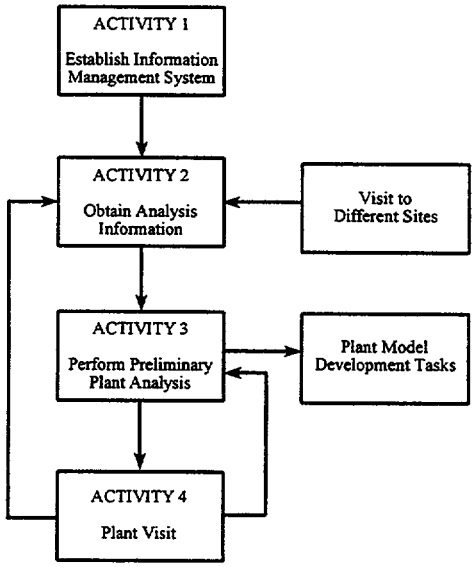


Figure 2.2 Activity relationship for plant familiarization analysis

The first activity, Establish Information Management System, involves the development of the database of the documents and a document distribution log methodology consistent with the guidelines provided in the project's QA program. This database will help to keep track of the vast amount of plant information obtained and to ensure that the latest and most appropriate

information is used consistently throughout the study.

The second activity, Obtain Analysis Information, involves obtaining specific information. Although this guide concentrates on the type of information needed for performing an internal event analysis, preliminary information needed for conducting internal fire, internal flood, and seismic analyses is also listed. This information comes from several sources, including the plant.

The next activity involves using the data to perform a preliminary plant analysis to initiate preparation of other tasks of the PRA, followed by a plant visit (Activity 4). The plant visit is scheduled to resolve questions, confirm and corroborate information already received, and obtain additional information. The process is iterative and the plant visits selective as discussed in Activity 4 (Section 2.2.2.4). More visits may be necessary for obtaining additional information found lacking as a result of the ongoing analysis or as the program matures. For example, it would be manpower intensive and cost prohibitive to conduct during the first visit a spatial interaction study (see Section 8.3) to assess likely fire scenarios before dominant accident sequences for internal events have been appropriately quantified and evaluated.

2.2.2.1 Activity 1 - Establish Information Management System

A large amount of plant information is collected from different departments of the plant owner including those from the designer, the architect-engineer, the builder of the plant, as well as from different departments within the plant. The information is then organized and selected copies are distributed to the PRA team members. To verify that the information is properly integrated and documented, a formal system for information and data acquisition and tracking is established. The database structure should contain sufficient detail for including revision number, date and title of individual drawings and procedures, as well as listing the team members and organizations that possess a working copy (or the original) of the material. A person should be assigned (usually by the project manager) to keep track of all requests for additional information, for cataloging the data, and for controlling the flow of information within the project. The team is expected to communicate continually with all the information sources throughout the project. Successful data management will ensure that the latest information is provided to the team members in a timely manner and used consistently throughout the project.

The team leader for the PRA project is responsible for establishing and maintaining the IMTS. The team leader should ensure that this system is established prior to or soon after the project is initiated. At the beginning of the project, points of contact should be identified within the participating organizations for acquiring and distributing material.

The IMTS should help to facilitate the timely distribution of current plant information to project team members. It should also establish an organizational structure showing lines of responsibility for the maintenance of a project information filing and data retrieving system.

The information referenced in the IMTS should include all documents, analyses, or drawings that may be used in the performance of the PRA. This information can be categorized as:

- plant drawings (flow diagrams, instrumentation and control diagrams, plant layout drawings, cable routing diagrams, etc.),
- procedures (regarding normal operation, abnormal operation, system tests, emergency operation, etc.),
- plant data (maintenance records, test records, scram records, test schedule, transmission line outage information, etc.),
- data from other plants (information on which to base generic data distributions)
- design information (loss-of-coolant accident [LOCA] analysis results, success criteria calculations, design bases, etc.), and

- training material (operator training material, system engineer training material, etc.).

To help control the flow of information, the IMTS should contain, as a minimum, the following data elements:

- a unique reference number for each item,
- date the item was received,
- item source,
- item title,
- item revision number,
- item issue date,
- a key to the item's distribution within the project team, and
- a data element reserved for comments.

It is useful to keep track of how and where documents have been distributed within the project team. In addition, it may be useful to reduce the amount of copying by identifying distribution categories. For some types of information, it may be sufficient to pass on to selected team members only a copy of the transmittal letter rather than a full report. Team members are then made aware of the availability of various information without being unduly burdened with possessing an excessive amount of material that may not be directly relevant to their particular tasks.

The "comments" section allows the project manager to annotate selected entries in the IMTS. For example, if a document having assigned a reference number "K18" is received that is an update of a previously received document "K2," then a comment can be added to the two entries in the IMTS:

- For K2: replaced (or augmented) by K18.
- For K18: replaces (or augments) K2.

A spreadsheet format, or any other database approach, is appropriate for the IMTS, so long as it is updated by the team leader (or some other designee) and a copy distributed periodically to other team leaders.

2.2.2.2 Activity 2 - Obtain Analysis Information

Plant-Specific Information

Table 2-1 lists plant documents that should contain information needed for conducting a Level 1 PRA. A brief description about each document and the relevant PRA information each may contain is also given in the table. Much of this information can be obtained prior to any plant visit. However, before any specific documents are requested, the project team should be made aware of all the possible plant documents that may contain the information indicated and then selectively request those deemed most appropriate for the project. In particular, a list of piping and instrumentation diagrams should be provided to the team and copies be made available of those diagrams considered most relevant by the team.

It is essential to have a senior member of the plant staff act as a contact point for obtaining plant information from each source. This person should: (1) be familiar with the process of acquiring the types of information listed in Table 2-1, (2) provide the indices for the documents and possibly give sample documents to the PRA team at the beginning of the information gathering task, (3) be able to understand why the information is needed, and (4) continue to serve as liaison throughout the project. It is likely that several different organizations or groups within an organization will be asked to provide information or other support for the PRA. The idea behind requesting a "senior member" as a permanent point of contact is to facilitate and expedite the requests for information made to these different groups.

It is important to ensure that the most up-to-date information is used in the study. Before a document is requested, it should be known how often it is updated and whether portions of the document are out of date. Close communication is essential between the PRA team leader and the designated senior plant staff member at the information source for assuring that the requested plant information is up to date.

Table 2-1 Plant information needed to perform a Level 1 internal event PRA

	Plant Document	Information Provided
1	Final Safety Analysis Reports	General description of the plant, systems, and design basis accidents submitted to the regulatory agency
2	System Descriptions, System Manuals, Equipment Manuals (manufacturers)	Detailed system descriptions (possibly used in operator training), operating envelope and success criteria
3	Piping and Instrumentation Diagrams, System Flow Diagrams	Schematics of systems showing piping specifications, components, instrumentation sensors, and flow paths
4	Elementary Diagrams	Control diagrams for components
5	Electrical One-line Diagrams	Showing breakers and components that are connected to different electrical buses and motor control centers, control logic
6	Equipment Layout Drawings	Showing location of major components in different plant areas, to determine accessibility to areas of recovery and potential common cause effects
7	Emergency Procedures and other procedures that help the operators during an accident	Accident scenario development, human reliability analysis, accident mitigation strategies for event tree development
8	Operating Procedures	Full, low power and shutdown activities
9	Training Procedures for Mitigating Accidents	Accident scenario development, human reliability analysis
10	Test and Maintenance Procedures for Major Equipment, Surveillance Procedures	Low power and shutdown activities, system availability, corrective and preventive strategies
11	Maintenance Logs	Maintenance unavailability data, mean-time-to-repair, failure frequency
12	Licensee Event Reports	Incident reports that are required to be submitted to the regulatory body, initiating event source book
13	Technical Specifications and Other Regulatory Requirements	System model development, limiting condition of system operation, allowed down times
14	Plant Incidents and Analysis Reports, Scram Reports, Operator Logs	Description and analysis of incidents at the plant that may or may not be reported to the regulatory body, recurring problems
15	Piping Location and Routing Drawings	Routing of piping throughout the plant
16	Analyses and Experiments Pertinent to the Determination of Mission Success Criteria	Documentation of experiments and thermal hydraulic analysis that were performed to address safety or operational issues, and plant behavior in specific conditions
17	Failure Mode and Effect Analysis	Detailed documentation of potential failure modes of equipment and their effect on the rest of the plant
18	Control Room Instrumentation and Control Layout Drawings	Layout of individual gauges, annunciators, and control switches in the control room
19	Descriptions of Known Safety or Regulatory Issues to Be Addressed	Potential failure modes and accident scenarios, level of detail of PRA model needed

Generic Information from Similar Plants

Analyses performed for similar plants can also be very useful. It can enhance the completeness of the PRA model by providing supplemental information on: the reliability of similar plant components, potential accident initiators, potential accident scenarios, and common safety issues. Six types of generic information that can be considered useful for supplementing the PRA are listed in Table 2-2 along with some selected examples. As a part of the information gathering task, a compilation of the information in the table should be performed.

Table 2-3 lists all the tasks required for conducting an internal event analysis and cross references each task with the needed information listed in the previous two tables.

Table 2-2 Generic information from plants of same/similar design

	Generic Information from Plants of Same/Similar Design	Examples
1	PRAs	Novovoronez PRA
2	Analysis of Experienced Events	IAEA-TECDOC-749 on Generic Initiating Events for PRA for VVER Reactors
3	Thermal-Hydraulic Analysis	
4	Component Failure Data Analysis	IAEA-TECDOC-478 on Component Reliability Data Sources in PRA
5	Accident Scenario Description/Analysis	
6	Regulatory Documents Dealing with Various Issues	

Information Needed for Internal Fires, Internal Floods, and Seismic Events

Table 2-4 lists the plant information needed for an internal fire analysis.[1] Table 2-5 lists the information needed to perform an internal flood analysis. Basically, plant-specific flood incident data, potential sources of flood, and pathways from the flood sources to plant equipment are needed.

Table 2-6 lists the information needed to perform a seismic event analysis. The information is needed to determine the seismic hazards at the plant site and the component fragilities. A hazard analysis provides curves that present the frequency of occurrences of seismic events for a range of ground-motion intensities. A fragility analysis provides component and structure fragilities that are used to calculate the likelihood that the component or structure will fail, given a seismic event of a certain magnitude.

[1]Note that in the U.S., information relevant to this table comes from the plant's implementation of the regulatory requirements specified in Appendix R of 10CFR50. The Appendix R submittal contains: the definition of fire areas, including the fire protection equipment; safe shutdown analysis that assures that a minimum set of plant systems and components are available to shutdown the plant, given a postulated fire with a concurrent loss of offsite power; and combustible loading analysis that identifies the sources of combustibles, including transients and cables. For a fire PRA, in addition to the Appendix R submittal, plant-specific and generic fire incident data and cable location and routing drawings are needed. The noted table summarizes the information needed from those plants that do not have an Appendix R submittal or its equivalent.

Table 2-3 Cross reference of PRA tasks and plant information needed

PRA Tasks	Plant Specific Information/Documentation Needed (Items from Table 2-1)	Generic Information for Plants of Similar Design (Items from Table 2-2)
Familiarization	All	All
Sources of Radioactive Releases	1,2,6,19	1,2,5,6
Select Plant Operating States	1,2,8	1
Definition of Core Damage	16	1,3
Selection of Initiating Events	1,2,7,9,12,14,17,19	1,2,5,6
Definition of Safety Function	1,2,7,9,14,16,19	1,2,3,5,6
Function/System Relationship	1,2,7,14,16,19	1,2,5
System Requirements	1,2,3,4,5,6,7,13,14,16,17,19	1,2,3,5,6
Grouping of Initiating Events	1,2,3,4,5,6,7,13,14,16,17,19	1,2,5
Event Sequence Modeling	1,2,6,7,9,12,14,16,19	1,2,3,5,6
System Modeling	1,2,3,4,5,6,7,13,14,16,17,19	1,2,4
Human Performance Analysis	1,2,6,7,9,12,14,16,18	1,2,5,6
Qualitative Dependence Analysis	1,2,3,4,5,6,7,19	1,2,5,6
Impact of Physical Process on Logic Model	1,2,7,9,12,14,16,17,19	1,2,3,5,6
Plant Damage State	Information needed for preceding tasks that provide input to the task	1,3
Analysis of Initiating Event Frequency	1,2,7,9,12,17,19	1,2,5,6
Component Reliability and Common Cause Failure	10,11,12,19	1,2,4,5,6
Assessment of Human Error Probabilities	1,2,6,7,9,12,14,16,18,19	1,2,5,6
Accident Sequence Boolean Equations	1,2,3,4,5,6,7,13,16,17,19	1,5
Initial Quantification of Accident Sequences	Information needed for preceding tasks that provide input to the task	1,4
Final Quantification of Accident Sequences	Information needed for preceding tasks that provide input to the task	1,4
Uncertainty Analysis	Information needed for preceding tasks that provide input to the task	1,4
Importance and Sensitivity Analyses	Information needed for preceding tasks that provide input to the task	1,5

Table 2-4 Information needed for internal fire analysis

Fire Area Definition - Areas separated by 3-hour rated barriers
Fire Barriers - Fire doors, fire walls, cable penetrations, cable tray insulations
Loading of Combustibles and Their Physical and Combustion Properties - Cables, lubricating oil, paper, etc.
Cable Location, Separation, and Routing Drawings - Power cables and control cables
Plant-Specific and Generic Fire Incidents Reports
Fire Detection Devices - Smoke detectors, heat sensors
Fire Suppression Devices - Sprinklers, CO_2, halon system, fire hydron, fire hose, fire extinguisher, deluge system
Fire Contingency Plans - Emergency procedures in case of a fire.
Safe Shutdown Analysis - Analysis demonstrating that a fire postulated at a given location can be mitigated with the plant brought to a safe shutdown condition.
Breaker Coordination Study - Studies indicating that the sequencing of the breaker opening and closing during a postulated fire will not adversely affect the plant's ability to mitigate the fire.

Table 2-5 Information needed for internal flood analysis

Potential Sources of Floods - Storage tanks, lakes, rivers, oceans, reservoirs, their location, elevation, and volume
General Arrangement Drawings - Showing the plant site topography information and the proximity of plant structures to nearby flood sources
Potential Path Ways Between the Sources of Flood and Plant Buildings - Piping, pipe tunnels, floor drains, doors, dikes, cable tunnels
Interconnections between different floors and buildings - Doors, dikes, floor drains, pipe tunnels, cable tunnels
Plant Specific Flood Incident Descriptions and Analyses
Emergency Procedures for Floods (and procedures for responses to high sump levels)

Table 2-6 Information needed for seismic analysis

(a) Information for Performing Hazard Analysis

Type of Information	Desirable Information
Seismicity around the region	• Documents on historic earthquakes in a wide area surrounding the site • Documents on recent earthquake activities around the site • Documents/references related to the siting of the plant • References on the seismological studies for the region (e.g., magnitude, attenuation) • Recorded ground motions (if not available, use U.S./European records for similar grounds)
Geological and ground survey (if the site is near the ocean, include seabed survey)	• Geological maps; wide area (1/100,000 ~ 1/200,000), vicinity (1/1,000 ~ 1/5,000), and vertical geological cross-section map • Aerial photographs (if any) • Topological surface survey (existence of lineaments/dislocations) • References on the seismic geostructure around the region (seismotectonics) • Survey on the active faults around the region (e.g., fault length, dislocation speed)
Local Soil Condition (the information is also used in fragility analysis)	• Boring/pit/trench survey results • Soil column profile • Survey on groundwater • Shear wave velocity data (if any) • Laboratory/In-situ test results on rocks and soil

(b) Information for Performing Fragility Analysis

Type of Information	Desirable Information
Documents on Structural Design	• Architectural/structural drawings for buildings and components • Engineering specifications on material, fabrication and construction • Design codes/standards used in the plant design • Any material test results (e.g., concrete cylinder tests, foundation bearing tests). • Records on the structural analyses including analysis models
Information on Component/Equipment	• Design drawing of components (e.g., support/frame/panel, electric circuit diagrams) • Any available vibration test results • Details of anchorage and related design code/standard • Generic information on the seismic fragility of component/equipment • Records on failure/repair on equipment
Other Information	• Any structural analysis performed for the plant (e.g., seismic analysis of reactor building, integrity analysis of vessels/piping). • Past records on the structural integrity (e.g., cracks, rusting, settlement and past repair works) • Availability of supply systems (offsite power, water)

2.2.2.3 Activity 3 - Perform Preliminary Plant Analysis

Preliminary analysis of the information gathered will verify that the necessary information is available and will identify additional information needed. The analysis also allows the information to be organized as inputs to subsequent project tasks. The following descriptions specify the output of the preliminary information analysis. It is expected that the specified information may not be readily available and significant effort may be needed to obtain the information. It is up to the team to decide how complete the information has

to be before proceeding to the subsequent tasks. The gathering of this information can be considered the initiation of the remaining PRA tasks. The task leader for each of the tasks will be responsible for the preliminary analysis.

Review of Information from Similar Plants - Any generic information listed in Table 2-2 that is collected should be reviewed for applicability to the current PRA tasks. A description of the potential use of each item should be given by the task team. The items in the table may provide insights into potential unique accident scenarios or failure mechanisms. For example, a review of the Novovoronez PRA might find that failure of the reactor coolant pump seal leading to a LOCA is an important cause of core damage and may have to be considered in the present analysis. Analysis of the issue of the vulnerability of pump seals to LOCA conditions should then be performed, taking into account plant-specific design features, to determine applicability. Once an issue is identified as applicable, how it can be modeled in the PRA should be described.

Initiating Event Analysis - The plant incidents that are potential accident initiating events should be reviewed and tabulated. For each incident, the following should be noted: the date, time, and plant condition when it occurred, its impact on plant systems, causes, sequence of events leading to its termination, and changes in plant design and operations that resulted from it. Discussions of other possible causes of similar events would also be useful.

Data Analysis - Reported failures on plant components should be tabulated, including: the cause of failure, how the failure was detected, the plant's condition, the repair time, and the effects of the failure on the plant. To quantify the failure probability, the following information is also needed: the number of times the component is used or challenged, the number of similar components at the plant, the test and maintenance strategy, and the time period of the collected data.

System Analysis - A listing of frontline systems that can potentially be used to mitigate the progression of probable accidents started by an initiating event and a listing of support systems including those that provide automatic actuation signals should be prepared. The listing should include one paragraph summaries describing the function of each system, the number of trains in each system, the function(s) each system performs, and the system's design capacity. A top-level matrix indicating the system and support system dependency should be prepared. Information on train-level and component-level dependencies and setpoints for automatic signals should be collected as well.

Success Criteria Determination - References to existing thermal-hydraulic analyses that determine the timing of potential accidents and success criteria of the systems employed in the analysis should be compiled. This compilation will help to determine if any additional supporting thermal-hydraulic analysis is needed at this stage of the study.

Event Tree/Accident Scenario Development - Event sequence diagrams based on the relevant emergency procedures for transients, loss-of-offsite power, and LOCAs should be developed. The mitigating functions and the systems associated with the functions should be tabulated.

Human Reliability Analysis - Relevant emergency procedures should be listed. Diagrams of the detailed layout of instrumentation and controls in the control room should be obtained/prepared and diagram identifiers tabulated. A review of the equipment layout drawing of various buildings should produce simplified system drawings indicating the physical location of key components that may be needed for manual, emergency operation.

2.2.2.4 Activity 4 - Plant Visit

Usually, the initial plant visit should take between three to five days. Ideally, the entire PRA team should participate in the visit. This allows all team members to become familiar with the design and operation of the plant and become acquainted with key personnel. This first visit should occur after the team has had a chance to provide a preliminary analysis of the material requested. The plant visit then provides an opportunity to confirm what the information conveys, why it is needed to perform a PRA, and to clarify any outstanding questions. Questions and the types of pertinent information needed for the plant visit should be sent to the plant ahead of time so that the visit becomes highly focused. It would be

helpful to pre-arrange for communication devices that allow for easier communication during plant walkdowns in noisy areas. To optimize the available time at the plant, an agreed-upon agenda and schedule of areas to visit should be prepared and followed.

The plant visit generally consists of the following activities:

1. Discussions[2] with plant engineering and operational staff concerning:
   - normal and emergency configurations of the various systems of interest,
   - normal and emergency operation of the various systems during various accidents as outlined by the analysts,
   - system interdependencies,
   - design changes implemented at the plant,
   - automatic and manual actions taken in response to various emergency conditions,
   - operational problem areas identified by plant personnel that might have a potential impact on the analysis,
   - subtle interactions and failures identified by the analysts (or from past studies) that might be applicable to the present study, and
   - detailed discussions regarding emergency procedures, including walk-throughs of various accident scenarios.
2. Discussions with plant engineering and maintenance staff concerning:
   - data (maintenance logs, licensee event reports, etc.) on specific items provided by the team leader to the data analyst, and
   - implementation of test/ maintenance procedures.
3. Discussions with the plant staff concerning training practices for various emergency conditions.
4. A visit to the plant simulator (if possible) where the operators perform various accident scenarios, as outlined by the analysis team.
5. A tour of the plant focusing on the systems modeled, noting such things as:
   - location of equipment (e.g., elevation),
   - room accessibility (with or without doors),
   - type of doors (e.g., flood, fire),
   - room size,
   - natural ventilation conditions, and
   - travel time for operators.
6. A tour of the control room, noting such things as:
   - relative location of panels,
   - layout of instrumentation on the panels,
   - type of instrumentation on the panels,
   - relative location of emergency procedures in the control room,
   - type of controls for system and component actuation on the panels (e.g., buttons, switches, key-locked switches, etc.),
   - type of annunciators and location on panels, and
   - annunciator indication.

After the additional information is obtained during the plant visit, the outputs of the preliminary plant analysis task (as described in Activity 3) should be finalized to the extent possible before being employed in subsequent tasks in the PRA. The plant information gathering effort continues throughout the PRA study so that a coherent PRA model is developed that reliably reflects the plant design and operation. Frequent communications between the PRA team and the point of contact at

[2]Discussions are documented where required. It should be noted that not all analysts participate in every discussion nor visit every plant area, e.g., control room access is usually very restricted.

the plant is expected. Requests for additional information and additional plant visits focusing on specific subjects is expected.

Examples of possible subsequent visits are the following. One visit could be a walkdown of the plant from a spatial interactions/internal plant hazards perspective; a second (and possible additional) visit(s) could focus on interacting with plant operators to help develop or validate the plant response models. Interaction with the operators to facilitate the quantification of operator actions is desirable. It is conceivable that additional effort at the site will be necessary to collect the desired plant-specific data. Each visit will have a focused goal, and, therefore, the makeup of each plant visit team will be tailored for that objective.

In practice, it is likely that formal visits are supplemented by frequent informal communication between the PRA team and the plant. A point of contact, who is very familiar with the plant operation, should be appointed as a point of contact on the plant side to coordinate information requests.

2.3 Products

As identified in Figure 2.1, the current task provides significant information to all analytical tasks of the PRA. In addition, the task will provide basic information needed for the final documentation. Specifically, the work products for this task are provided below:

- An IMTS will be developed and maintained throughout the life of the PRA.
  - The IMTS will include a database of the documents and a document distribution log methodology consistent with the guidelines provided in the project's QA program. This database will help to keep track of the vast amount of plant information obtained and to ensure that the latest and most appropriate information is used consistently throughout the study.
  - The IMTS should help to facilitate the timely distribution of current plant information to project team members. It should also establish an organizational structure showing lines of responsibility for the maintenance of a project information filing and data retrieving system.
  - The information referenced in the IMTS should include all documents, analyses, or drawings that may be used in the performance of the PRA.
- A letter report documenting the outcome of the plant visit is sent to the various organizations. This allows the utility personnel who have been queried to clarify any misunderstandings and provide traceability of the information received.
- After the additional information is obtained during the plant visit, the outputs of the preliminary plant analysis task (as described in Section 2.2.2.3) should be finalized to the extent possible before being employed in subsequent tasks in the PRA.
- The plant information gathering effort continues throughout the PRA study so that a coherent PRA model is developed that reliably reflects the plant design and operation. Requests for additional information and additional plant visits focusing on specific subjects is expected.

3. DOCUMENTATION

The objective of this task includes all aspects of documentation of the probabilistic risk assessment (PRA). "Documentation" here is understood in its broad sense; that is, all reports and data files created during the PRA as well as those procedural steps that influence the form and handling of documentation. The Documentation task is another activity associated with the project administration component of a PRA (refer to Figure 1.1). Figure 3.1 shows the important relationships between this task and the other major tasks of the PRA. These relationships are discussed below in Section 3.1.

The primary objective of the PRA documentation should be to fulfill the requirements of its users and be suitable for the applications that will follow. This means that it is important to identify potential users and uses of the PRA early on, structuring the documentation to best serve the users, to support peer review, and to permit continuing or even changing use.

This discussion on documentation has, therefore, been divided into two broad parts dealing with documentation structure and products for the Kalinin PRA. After the section in relation to other PRA tasks, the structure of PRA documentation is discussed (Section 3.2) in general terms. In this section, brief descriptions of the various documentation levels that are needed for various identified audiences are provided. These attributes are then translated (in Section 3.3) into a description of the documentation (or PRA products) that will be developed as part of the PRA for the Kalinin Nuclear Power Station.

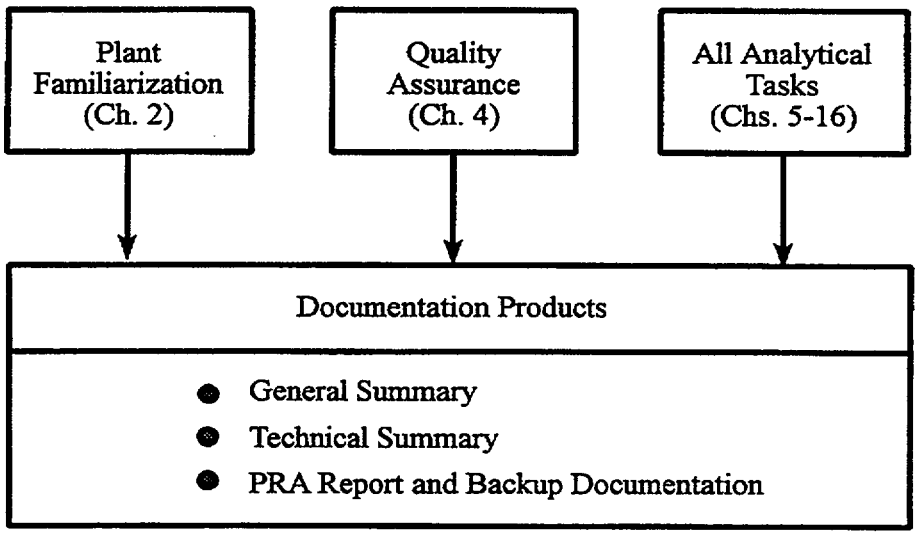


Figure 3.1 Relationships between documentation and other tasks

3.1 Relation to Other Tasks

As identified in Figure 3.1, the current task requires information from all of the PRA analytical tasks. In addition, information is needed from the Plant Familiarization (Chapter 2) and Quality Assurance (Chapter 4) tasks.

3.2 Documentation Structure

PRA is a scientific and engineering analysis performed for many purposes. It is a source of knowledge of plant behavior, providing an understanding of the integrated response of the nuclear plant to upsets of many types. It is a source of knowledge of plant safety providing an understanding of the risk posed by the operation of the plant. It is a management tool allowing

operators and regulators to test the risk impact of alternative strategies. It can also provide information to government officials and the public, enhancing policy decisions. It is much more than a technical analysis for use by the technical community alone.

PRA documentation offers a unique set of problems–how to present the results of an extensive scientific and engineering analysis of the integrated performance of a large, complex system in terms accessible to experts n risk assessment, plant operators, engineers and managers, plant designers and vendors, regulators at the local and national levels, government officials and other interested parties. Because of the broad scope of the analysis itself, the authors are driven to tell everything they have learned and accomplished. This often leads to massive documentation that only they can follow. The published documentation, however, is a product whose success is judged by its ability to meet specific objectives, rather than by its mass.

The best approach for developing the documentation is to identify the principal audiences and the desiderata of documentation for each audience; that is, what are the needs of each audience and what should the audience carry away from reading the documentation. Documentation can then be developed to meet those desiderata as succinctly and clearly as possible. The test for inclusion of material developed during the study is simple: is it necessary to meet the reader's needs?

For the Kalinin project, the following audiences should be considered in developing the documentation:

- General Audience. Non-technical government officials, non-technical managers, and perhaps the general public.
- Technical Community. Engineers, scientists, technical workers, and managers in government and industry with a technical understanding but without any specific experience or an understanding of PRA.
- PRA Community. Engineers, scientists, technical workers, and managers with PRA knowledge and experience (i.e., users of PRA results).
- Kalinin Risk Managers. The PRA team for Kalinin, people who will actually make calculations using the Kalinin PRA for the plant operator, the regulator, or another body.

Table 3-1 lists the desiderata for documentation for each identified audience.

3.3 Products

It is natural and important to define the reports that document the PRA in top-down fashion as presented in Table 3-1. However, preparation of the documentation occurs in reverse order, beginning with the detailed information gathering, calculation sheets, model construction, and computer work. This material is formally documented in task reports that become appendices to the PRA Report. These details, in turn, are abstracted and reorganized into the main body of the PRA Report. The entire PRA Report is used to recast the model and results into the Technical Summary for a competent technical audience that lacks PRA and, possibly, nuclear power plant experience. Finally, the General Summary presents key results and insights from the work summarized for a nontechnical audience.

The objective of this section is to define the documentation for the Level 1 PRA done for the Kalinin Nuclear Power Station for internal initiators (including fire and flood) and seismic events. Documentation for a Level 2 and Level 3 PRA are described in Part E of this volume.

3.3.1 General Summary

The General Summary is organized from the results presented in the Technical Summary and PRA Report. It is essential for the report to be understood by non-technical government officials, non-technical managers, and perhaps the general public. It must, therefore, be concise, interesting, and written in lay language so that a general

Table 3-1 Desiderata for PRA documentation for each identified audience

Desiderata	Comment
General Audience	Call this report the General Summary
1. Gain confidence in the analysis a. Analyst credentials b. Method validity c. Balanced presentation	1. Cannot be accomplished through the published report alone. Should be supported through involvement in the PRA process and personal interactions. (Parker et al., 1994)
2. Read and understand the report	2. Implications a. Clear and concise, limit to 15-20 pages b. Simple description of plant, normal operation, and potential upsets c. Simple description of the basic methodology d. Refer reader to more detailed documentation
3. Understand the risk and the risk management process	3. Implications a. Present risk in lay terms and explain why reasonable b. Explain potential uses
Technical Community	Call this report the Technical Summary
1. Capture interest	1. Provide a simple, thought-provoking introduction, i.e., attach the General Summary
2. Motivate scientists, engineers, and technical engineers to use the PRA	2. Present risk results in clear technical terms a. Display plant model in a format that emphasizes engineering knowledge imbedded in the analysis; an event sequence diagram approach is suggested b. Display the risk results in a format that emphasizes the important scenarios of importance and their special characteristics c. Avoid overemphasis on event trees, fault trees, and statistics d. Avoid impression that PRA is merely a statistical exercise
3. Provide training to the reader	3. a. How the plant works 1. Basic plant design, summary of safety systems and support systems, how they interact 2. Summary of upset conditions 3. Identify redundancy in function, equipment, and procedures 3. b. Risk management 1. What the PRA does 2. What is the risk 3. How severe accidents progress 4. How to develop strategies for risk management
4. Provide useful information for plant management	4. Information and uses a. Scenarios (equipment and human failures, their causes, and the relationships among them) that define the risk b. Support basic risk management calculations c. Provide basis for risk mitigation course for operators d. Permit placing new issues in proper risk perspective e. Provide traceable links to more detailed documentation

Table 3-1 Desiderata for PRA documentation for each identified audience (Cont'd)

Desiderata	Comment
PRA Community	Call this report the PRA Report
1. Summary of results and approach	1. Provide a simple, thought-provoking introduction, i.e., attach the General and Technical Summaries
2. Clear documentation of methods, results, models, and potential uses	2. The main body of the PRA Report serves two purposes a. Provides a thorough overview of the PRA, its models, its data, and its results, including simplified presentations of event trees and fault trees b. Guides the reader through the massive documentation in the appendices and in the Backup Documentation (see below), while stressing the connections between different parts of the documentation, e.g., the seismic analysis appendix is based on extensive information developed in the systems analysis, the event sequence modeling, and the human reliability appendices
3. Thorough documentation to support review and recalculation of results for risk management purposes	3. Appendices will include detailed fault trees and event trees, detailed reports on all tasks, all data, etc., and provide traceable links to the Backup Documentation
Kalinin Risk Management	This is the Backup Documentation: models, calculation files, working notes, technical information gathered in the task Plant Familiarization and computer programs and files
1. Clear documentation of methods, results, models, and potential uses	1. Document all notes so that an independent PRA expert can follow, understand, and replicate the work
2. Ability to perform risk calculations	2. Fully operational, complete risk model on computer a. All event trees and fault trees b. All data, generic and plant-specific c. Documented and verified computer code that can recalculate risk quickly following changes to the model or data
3. Full understanding of basis	3. Save and file all supporting information used in the PRA a. All hand calculations b. Raw data c. Background information (plant reports, previous analyses, procedures, meeting notes, etc.)
4. Ability to find documentation	4. Effective filing and retrieval system a. PRA Report must point to Backup Documentation b. Computer-based retrieval system must permit searches based on keywords and topics

audience can gain confidence in the analysis and understand risk and the risk management process. The General Summary for the Kalinin PRA is published as part of Volume 1 (i.e., the Project Summary) of this report.

3.3.2 Technical Summary

A desirable characteristic of a probabilistic approach to safety is that concerns (new, previously unanticipated concerns, as well as old ones) can be placed in their proper perspective with respect to possible consequences and likelihood. The presentation format that should be used for the Technical Summary should go even further, breaking down the frequency into two parts: the frequency of finding the plant in some degraded state and the chance of damage, given that condition. Note that this provides a structure for displaying the safety significance of conditions that have already been identified in safety analysis reports and the PRA. Furthermore, when new issues arise from other sources, they can be inserted into their proper place in the structure and judged accordingly. This ordering may help the technical community to understand the "riskiness" of various preaccident and accident conditions and to provide a basis for comparison.

A format that serves this purpose was recently developed to enhance the use of PRA information at a U.S. Department of Energy (DOE) reactor site (Bley et al., 1992). It defines a useful document quite different from many PRA technical summaries that have been done in the past. The rationale for this approach arose when a PRA had been published and used to address several specific safety design issues for the DOE reactor. In spite of the availability of the PRA, its widespread use for evaluating the safety for restart purposes was hampered by the mystique surrounding its traditional presentation of models and results.

In attempting to answer questions, such as "Why do I believe this reactor is safe to restart?", the DOE tried to use the PRA and decided that something more was needed to make the results generally accessible and clearly relevant to the day-to-day questions about the safety importance of each new issue. The basic goal became to develop a new top-down presentation format for the existing PRA, a format that could speak clearly to engineers, scientists, and managers who have not directly participated in the PRA and who may not be intimately familiar with the design and operation of the reactor. More formally, the objectives were to:

- Provide an easy-to-understand, simplified summary of reactor upset conditions, their likelihood, and the plant's capability to return safely to a stable state.
- Identify redundancy in function, equipment, and procedures.
- Consider the plant configuration as expected at restart, including all requirements of the safety evaluation report.
- Provide an alternate assessment of the effectiveness of the safety evaluation report in ensuring a safe plant configuration.
- Provide a risk-based tool that would assist in addressing new issues raised by any party by placing the issues in proper perspective, e.g., verifying the safety adequacy of new test programs, new procedures, training programs, and technical specifications.
- Provide a PRA basis for training on reactor safety concerns and operations.

These objectives are similar to the goals of the Technical Summary for the Kalinin Nuclear Power Station PRA, which focuses on continued operation rather than startup. The Technical Summary for the Kalinin PRA is published in Volume 2 of this report.

3.3.3 PRA Report and Backup Documentation

The primary PRA documentation is the PRA Report and the Backup Documentation, i.e., the traditional documentation. The PRA can be no better than this documentation. Its usefulness and "reviewability" are defined by the PRA Report, its accessibility, and the ease of its linkages with the Backup Documentation. The following discussion of the PRA Report is based

primarily on IAEA (1992), McCann et al. (1985), and EPRI (1984).

The detailed documentation of the PRA should be well structured, clear, and easy to follow, to review, and to update. In addition, means should be provided for possible extensions of the analysis, including integration of new topics, use of improved models, broadening of the scope of the PRA in question, and use for alternate applications. Explicit presentation of the assumptions, exclusions, and limitations of extending and interpreting the PRA is also important to the users. Clear presentation of the qualified results should be given. It is also recommended that:

- Conclusions should be distinct and reflect not only the main, overall results but the contributing analyses.

- Emphasis should be given to the analysis of uncertainties in the data and to sensitivity analysis where the effects of assumptions, limitations, and conservatism in methods and modeling are clearly demonstrated.

The first step in organizing the documentation of the study consists of determining the nature and amount of information that is going to form the external documentation, i.e., what is going to be published and the information that is going to form the backup documentation.

The PRA Report should provide, within the report or by reference to backup material, all the necessary information to reconstruct the results of the study. All intermediate subanalyses, calculations, assumptions, etc., which will not be published in any external reports, should be retained as notes, working papers, or computer outputs. This is very important for reconstructing and updating each detail of the analysis in the future. It is recommended to use well-organized computer and word processor files as much as possible for storing this type of information.

The organization of the PRA documentation should be governed by two general principles:

1. Traceability: For reviewing and updating the analysis, it should be possible to trace any information with minimum effort.

2. Sequentiality: The order of appearance of the analysis in the final documentation should follow, to the extent possible, that of its actual performance--that is:

   - initiating events
   - event tree analysis
   - systems analysis and related topics
   - accident sequence quantification
   - uncertainty and sensitivity analysis.

It is recommended that the PRA Report be divided into three major parts:

1. Summary report[1]
2. Main report
3. Appendices to the main report.

The Summary and Main Report for the Kalinin PRA project have been published as Volume 4 of this report. The appendices are contained in Volume 5.

The summary report should provide an overview of the PRA project's motivations, assumptions, objectives, scope, results, and conclusions at a level that is useful to a wide audience of reactor safety specialists and that is adequate for high-level review. The summary report is also designed to provide a clear framework and guide for the reader or user before consulting the main report.

The summary report should include a subsection on the report organization that should present concise descriptions of the contents of the sections of the main report and the individual appendices. The relation between various sections and parts of the PRA should also be included in this section.

[1]Note that this is a summary of the PRA Report and is not identical to the Technical Summary (which for the Kalinin project is found in Volume 2 of this report) or the General Summary (which for the Kalinin project is found in Volume 1 of this report).

Outlines of the PRA Report and Backup Documentation are shown in Tables 3-2 and 3-3, respectively. Also given in the tables are the chapters or sections in these procedure guides which contain the tasks that produce the documentation. Because the report only highlights methods, models, and results, a thorough reference to the appendices and backup material is mandatory. Note that although some of the same material is identified for inclusion in the appendices of the PRA Report and in the Backup Documentation, the latter is the repository for all details, and the appendices are only to give detail that is assumed to be important enough for inclusion in the PRA Report.

The documentation done as the project tasks are being performed constitutes the appendices of the PRA Report. After each task is documented, a summary of that documentation is prepared. After the entire PRA is completed, the main report is prepared with the help of the summaries generated for each task. An Integrated Reliability and Risk Analysis System (IRRAS) database containing the Level 1 PRA model should be included as a supplement to the report in the form of diskettes. It should be complete with descriptions of basic events, systems, and event trees and allow easy reproduction of the results including uncertainty analysis and sensitivity calculations.

3.4 References

Bley, D. C., et al., "Management Experience Using a Novel Probabilistic Risk Assessment Format for Safety Communication," *Transactions of the American Nuclear Society*, June 1992.

EPRI, "Documentation Design for Probabilistic Risk Assessment," EPRI-NP-3470, Electric Power Research Institute, 1984.

IAEA, "Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1)," Safety Series No. 50-P-4, International Atomic Energy Agency, 1992.

McCann, M., et al., "Probabilistic Safety Analysis: Procedures Guide," NUREG/CR-2815, Rev. 1, Brookhaven National Laboratory, August 1985.

Parker, F. L., et al., "Building Consensus through Risk Assessment and Management of the Department of Energy's Environmental Remediation Program," Committee to Review Risk Management in the DOE's Environmental Remediation Program, National Research Council, National Academy Press, Washington, DC, 1994.

Table 3-2 Contents of PRA Report

Contents	Relevant Chapter in Procedure Guides
Summary Report	Chapter 3
Summary of Objectives, Scope, Participants	
Report Organization	
Summary of Methods Used	
Summary of Level 1 PRA Results	
• Core damage frequency	
• Dominant accident sequences	
• Important systems and components	
• Important operator actions	
• Important uncertainties	
Summary of Potential Applications of Level 1 PRA Results	
• Applications at the regulatory agency	
• Applications at the power plant	
Main Report	Chapter 3
Objectives, Scope, Participants	
Methods Used	
Level 1 PRA Results	
• Core damage frequency	
• Dominant accident sequences	
• Important systems and components	
• Important operator actions	
• Important uncertainties	
Potential Applications of Level 1 PRA Results	
• Applications at the regulatory agency	
• Applications at the power plant	
Summary Plant Description	
Accident Initiators and Plant Response	
• Accident Sequence Delineation	
• System Analysis	
• Sequence Quantification	
Appendices	

Table 3-2 Contents of PRA Report (Cont'd)

Contents	Relevant Chapter in Procedure Guides
Initiating Event Analysis and Quantification	Chapter 6 and Section 9.1
Functional Analysis and System Success Criteria	Section 7.2
Event Sequence Modeling and Plant Damage State Analysis	Section 7.3 and Chapter 15
System Analysis	Sections 8.1, 9.2, and 9.3
Human Reliability Analysis	Chapter 10
Qualitative Dependency Analysis	Section 8.2
Accident Sequence Quantification	Sections 11.1 and 11.2
Uncertainty, Importance, and Sensitivity Analyses	Sections 9.2 and 11.3
Spatial Interactions	Section 8.3
Fire Analysis	Chapter 12
Flood Analysis	Chapter 13
Seismic Analysis	Chapter 14
VVER Generic Database	Chapter 9

Table 3-3 Contents of backup documentation

Contents	Relevant Chapter in Procedure Guides
Backup Documentation	
Plant Description	Chapter 3
• Functions and related systems	
• Systems schematics and procedures	
• Emergency procedures	
Calculational Files	
Event Trees	Section 7.3
Fault Trees	Section 8.1
Human Reliability Analysis Backup Material	Chapter 10
Plant-Specific Database	
• Initiating event frequencies	Section 9.1
• Component failure rates	Section 9.2
• Common-cause failure rates	Section 9.3
• Test and maintenance unavailabilities	Section 9.2
• Human error probabilities	Chapter 10
Detailed Quantification Results	
• Accident sequence cutsets with quantification	Sections 11.1 and 11.2
• Importance measures	Section 11.3

4. QUALITY ASSURANCE

The objective of this task is to provide guidance for establishing a quality assurance (QA) program. The guidance provided should aid the project manager in the control of the activities needed to assure the technical adequacy of the probabilistic risk assessment (PRA) process and products. These activities include project organization, the technical analytical tasks, and documentation. The QA task is an another activity associated with the project administration component of a PRA (refer to Figure 1.1). Figure 4.1 shows the important relationships between this task and the other major tasks of the PRA. These relationships are discussed below in Section 4.1.

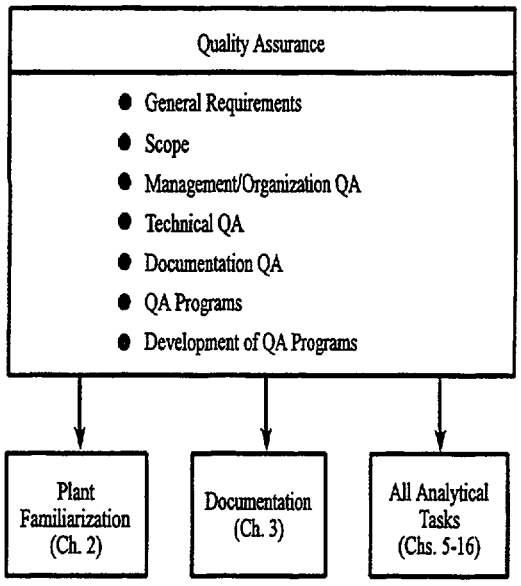


Figure 4.1 Relationships between quality assurance and other tasks

4.1 Relation to Other Tasks

In this task, guidance in the development of QA procedures is given by identifying the links between the PRA-related tasks in each of the programmatic areas (i.e., project organization, the technical analytical tasks, and documentation) and the QA characteristics (i.e., attributes, concerns, measures, standards) required to address the overall technical adequacy (or quality) of the study. A framework can then be structured where QA procedures for the PRA tasks can be formulated and an effective audit, review, and information-tracking system implemented.

4.2 Task Activities

Performing a PRA for a nuclear power plant entails extensive and detailed engineering and statistical analyses of complex systems and uncertain physical processes and requires the expenditure of considerable resources. These resources can only be justified by the belief that the PRA methodology, results, and conclusions provide valued input into decisionmaking by regulators and operators of these systems. Having a high degree of confidence in the PRA's accuracy and in its completeness is a necessary attribute for effective decisionmaking in addressing facility design, operational safety, and regulatory issues.

Because PRAs for nuclear power plants largely deal with highly improbable (or low frequency) events, the technical adequacy of the results from PRAs cannot be properly judged on the basis of real-life experiences. Evaluations that the study has generated conclusions that are both valid and relevant (i.e., technically accurate) are, therefore, more difficult. A technically adequate PRA is one that shows that the conclusions are well-grounded, correctly derived, justifiable, and that they are appropriate to the purpose(s) of the study.

Providing assurances on the technical adequacy of the PRA, on the effectiveness of the management of the PRA process, and that the end product is correct, usable, and fulfills the intent of the study requires the formulation and execution of a QA program.

4.2.1 General Requirements

A QA program for a PRA encompasses those project management activities that ensure that the analysts have followed the right procedure throughout the study, have made reasonable assumptions, discussed phenomena consistently, accurately portrayed system models, used commonly accepted databases and verifiable (or verified) codes, and documented results in a traceable fashion. Effective management contributes to the achievement of a technically adequate, or quality, product through its practice of in-depth analysis of what is required to perform

the PRA tasks, through identification of the skills required to perform these tasks, by the selection and training of the appropriate personnel, through the use of effective procedures for controlling/disseminating technical information and verifying results, and by the recognition of the responsibility of each team member (IAEA, 1992).

Development and implementation of QA procedures into the PRA tasks are tantamount to good management practices. Since the later phases of a PRA are dependent on the previous phases, execution of a PRA can be considered as a process. Resources should, therefore, be allocated throughout the study in a manner that ensures the highest quality of the end product. The Kalinin PRA project should view QA procedures as an integral part of the PRA process, and QA procedures should be a constituent part of the PRA tasks. Accordingly, the process by which quality of a PRA is assured is closely linked to the process by which the PRA is executed. The Kalinin PRA project should be structured and managed such that assuring quality of the PRA is not separated from the process of achieving each PRA task objective.

The QA program for this project should provide a disciplined approach to all activities affecting the quality of the PRA, including verification that each task has been performed satisfactorily and that necessary corrective actions are implemented when those QA standards, specified for a technically adequate PRA, are not being met. QA standards are based on the specifications and guidance given in the PRA procedure guides developed specifically for this project.

4.2.2 Scope

The major PRA procedural steps (IAEA, 1992) for which QA requirements should be specified can be generally classified as:

1. Management and organization
2. Identification of accident initiators
3. Modeling of accident sequence
4. Data assessment and parameter estimation
5. Analysis of plant systems
6. Quantification of accident sequences
7. Display and interpretation of results.

In the following tasks, there are specific guides for the PRA tasks connected with these major procedural steps that have been developed as part of the Kalinin PRA project. These guidance documents can be used in the development of specific QA requirements for conducting the PRA and for the QA standards needed for judging quality. In this context, the elements considered important in the achievement of a quality PRA (Garrick, 1984) are:

- a clearly defined objective and statement of purpose,
- a clear definition of the scope and depth of analyses,
- identification of the methodology to be used,
- qualification and commitment of the project team,
- timely progress reports on how methodology has been implemented,
- most important, a comprehensive review and technical evaluation program,
- a final report that is readable, believable, and with traceable results.

The essential ingredients for assuring quality are (EPRI, 1983):

- An understanding of the potential problem areas, or QA concerns, in performing each of the above-listed general PRA tasks that can affect the technical adequacy of the PRA study.

- The establishment of criteria, or QA standards, that incorporate the above-listed basic quality elements for judging the technical adequacy of the PRA study.

- The measures taken by the project management to ensure that the QA standards are being met.

Standards determine the methods that must be used, the reviews that should be taken, and the documentation that must be provided to ensure that the study is producing a technically adequate product. The actual mechanisms involved in implementing the standards, viz. the QA Program, should ideally show the connections between:

- who performs the reviews,

- when the reviews should be performed,
- the standardized check lists to be used, and
- the specific QA standards to be addressed.

The development and implementation of a QA program are a primary function of the PRA Project Manager, who must instill in the project team that quality is not considered a function that can be separated from the performance of any part of a PRA. The quality of a PRA is, therefore, normally judged by the adequacy of the methods used, how these methods were applied, how the resulting risk insights are conveyed and documented, and how the results have been utilized by the end user(s). Key factors in assessing the quality of the PRA include judgments as to how well the project has been planned and managed. There are steps that can be taken in the project organization, in the control of technical information, in the execution of the technical work, and in the documentation that will enhance or facilitate the achievement of quality. These are discussed in the following sections.

4.2.3 Management/Organization Quality Assurance

Providing assurances that a technically adequate product is being efficiently produced is a major goal of the project management. The planning/management task of the PRA project must be concerned with the definition of study objectives, the selection of a study team and methodologies, the formation of a management plan, the definition of a QA program, and the maintenance of a QA group. From a QA viewpoint, it is important to ensure that the project has been organized and planned to provide a proper level of experienced staff, a balanced allocation of resources, and a well-integrated, task-oriented process among the diverse tasks. Also important is that the project organization has implemented QA procedures and control points designed to assure that the PRA methods are being applied consistently, that the work remains focused on the study objectives, that the spending is under control, and that the work is on schedule. The project plan then becomes a standard for controlling the budget and schedule of a PRA and is an important contributor to quality.

The project planning must recognize that the appropriate use of risk-assessment methods and the technical information requires people that are both knowledgeable and experienced in the required disciplines. The authority of project and task leaders must be clearly defined to help assure that the right task team can be assembled. Experience has shown that the members of the study team have the following qualifications (Garrick, 1984):

- Experts in the analytical and probabilistic methods employed
- Nuclear engineers knowledgeable in the core- and containment-response phenomena
- Engineers who have hands-on knowledge in the operation of the power plant
- Specialists in environmental hazards, such as earthquakes, fires, and floods
- Practitioners who can translate analytical methods and plant knowledge into meaningful models for quantifying the risk
- Authors who have special skills in communicating highly technical and scientific work.

Well-defined responsibilities must be clearly articulated, and task interfaces identified by the project manager. Communication across these task interfaces is a very important element of a PRA study. When the task interfaces, lines of communication and task responsibilities are not clearly defined, and quality will be affected.

A well-defined project plan that contains a clear understanding of the purpose and objectives of the study can serve as a key management tool for providing direction and giving control to the risk study and the other elements of project management. For example, quality management should show that the scope of the PRA is consistent with the level of funding to avoid indefensible shortcuts for meeting budgetary constraints. The project schedule should be consistent with the staff's availability and level of

experience and should identify those points in the schedule where integration among the various tasks may be required and when internal reviews should be conducted.

The information transfer between the plant staff and the PRA study team and the necessary coordination and integration of the various PRA tasks make effective communication vital. A well-organized project is one where the flow of needed information by the various project teams is well managed. The project organization should identify specific individuals in the plant who can obtain the detailed information needed for the PRA study and who have sign-off responsibility for releasing this information in order to assure that the basic plant design and operational information given to the PRA team are both complete and correct. Also, an important part of the QA activity is the identification by the project organization of the qualified staff to review the plant and system models constructed by the study team.

Another key element in the quality management of information is the development and maintenance of a computerized database for the project documents and relevant technical information. QA procedures should be developed for controlling documentation. The procedure guides address this need. For example, the procedure guide for Plant Familiarization describes the requisite elements for an information management tracking system.

Reviews, which can take the form of internal checks or external technical and external oversight reviews, are an important technical element of a PRA. Each of these reviews can be effective in various ways in verifying or ensuring the technical adequacy of the study. Providing for conducting these types of reviews and formulating the ground rules needed to assure that the reviews apply completely and consistently to all tasks are important quality assurance activities that should also be performed by the project management. Guidance into the types of reviews and QA audit procedures is given in a later section.

4.2.4 Technical Quality Assurance

Central to the quality of a PRA is the methodology employed to perform the risk analysis and the implementation of that methodology, i.e., the *technical work*. The objective of a technical quality assurance program is to ensure that the work is complete relative to the stated objectives of the study, that the methodologies have been properly applied in a consistent manner, and that the calculations are accurate and yield consistent and reproducible results. The criteria often used in evaluating the quality of the technical work are: logical soundness, completeness, and accuracy. Logical soundness relates to whether the methodology can be justified by theory and whether the applications of the methodology violate any fundamental assumptions. Completeness relates to whether the technical work accounts for all relevant aspects of the study objectives, available resources aside. Accuracy relates to whether the technical work will produce a product that is sufficiently precise, free from possible biases, and sensitive to the untested assumptions. An accurate risk assessment must provide estimates of the risk consequences and uncertainties that are commensurate with the available data, knowledge in the operational states of the plant, and the understanding of the processes that can upset these states and their attendant consequences.

Key steps in the PRA methodology include: data and information handling, identification of accident initiators, plant/systems modeling, analysis of environmental hazards, and the quantification of the uncertainty in the various levels of risk measure. Some specific issues related to the quality of the technical work in these steps are discussed in the following paragraphs.

The quantification tasks of a PRA usually require the use of complex computer codes. There are several QA concerns. The capability of the code and the accuracy of the code output should be consistent with the desired application of the overall study. If the code has been changed to accommodate a desired application, the changes should be clearly indicated. It should be noted that they accomplish the desired result and are consistent with the overall structure of the code. Assumptions are usually made when using a code and in choosing from the various code options. These assumptions and choices should be clearly stated so that the accuracy of the assumption and the consistency in the options

chosen can be assessed. The preparation of the input deck is a task that can often introduce errors into the analysis. Accuracy in the input is an obvious major QA concern in PRA tasks involving code application. While the right methodology is necessary for quality, the lack of quality can be attributed to the misuse of the analytical tools. In this regard, there is the QA issue regarding the experience the study team has in the use of the code and in the interpretation of the results. Besides the methodology, it is the implementation of that methodology and its interpretation by mature analysts that helps in assuring a quality product (Garrick, 1984).

While identifying initiating events, it is important that the task procedures ensure that all the important events leading to core melt have been identified, that the sources used in identifying them are complete and accurate, and that the assumptions made in identifying and quantifying the initiating event frequencies are consistent. It is also important to consider the consistency of the grouping of initiating events regarding the same plant impact and the same set of safety systems required for shutdown.

Task procedures for developing event trees should be clearly stated, and the event tree methodology should be capable of addressing plant and operator responses completely. The procedures should be both internally consistent and consistent with the overall goals and scope of the study. Completeness and accuracy in addressing the definition of system success criteria are other QA concerns in event tree development. Dependencies between events in event trees require special techniques for quantifying the trees. The QA concerns about the quantification of dependencies are that all important dependencies be identified and calculated accurately. Also, the relationship between the top event of a fault tree of a plant system and the system success criteria must be accurately stated and consistently applied. The top event of each fault tree must correspond with the appropriate event tree event.

Crucial to the validity of the PRA study is the correspondence between the fault tree models and the actual plant systems, which should be both complete and accurate from a QA viewpoint. Many sources of information about the plant should be used in the support of the fault tree development to assure accurate and complete representation of plant systems, plant component failure modes (and rates), and their support systems. However, the level of detail should be consistent with the objectives of the study and with the availability of data needed to quantify the basic fault tree events.

The collection and interpretation of the required PRA data are essentially a subtask of the systems analysis task. This includes: failure rate information for components/systems, initiating event frequency data, basic human-error data, and information relating to test-and-maintenance procedures/intervals and repair times for systems and components. The procedures for collecting these types of data should be clearly stated and comprehensive in the methods recommended for data interpretation.

The quantification of uncertainty is fundamental to the notion of risk. The quality of the PRA is very dependent on how the uncertainties are classified and the rigor by which these uncertainties are systematically propagated through the plant logic models. A visible and logical treatment of uncertainty tells a great deal about the quality of the PRA. The QA concerns in the uncertainty quantification tasks are those of clarity, completeness, consistency in the procedures, and also accuracy in the analysis assumptions and applications.

In order to judge or control the quality of the PRA study, there must be standards of quality against which the study may be measured. Standards may be very general or very specific. If the standards are defined in broad terms, then the burden of the effort in establishing the technical adequacy of the task is placed on the QA reviewer. In contrast, if the standard is very specific, it is less susceptible to interpretation and is more suitable for the QA reviewer. A general standard, however, does not restrict or inhibit development of the state of the art as a specific standard might. The philosophy in defining standards is that they should be as specific as possible without unduly limiting the types of methodologies or PRA practices used. It is expected that the standards developed by the project management would be specific enough to serve as a checklist for assuring study validity, for

addressing the QA concerns discussed above, and be flexible enough to be modified if warranted. The QA of all the PRA tasks generally involves the review of interim study topics. As such, conducting the PRA requires the development of progress outputs that can serve as effective checks on quality. The discussions below on PRA documentation and quality verification will be helpful to the project in the development of the requisite standards and audit procedures.

4.2.5 Documentation Quality Assurance

The work involved in conducting a PRA requires the development of progress outputs that can serve as effective checks on quality. A well-conceived methodology and program plan can assure that intermediate deliverables are present and documented in a manner in which the output of one subtask meets the needs and requirements of other tasks, and the information provided can be easily utilized as the input to a subsequent PRA task. Examples of such intermediate deliverables include: data packages that become the basis for the PRA inputs, initiating events (both external and internal), and plant/system logic models that are the building blocks of the event sequence models. Documentation is then meant to include: in-progress documentation, models, calculation files, data files, and technical information. Chapter 3 (Documentation) provides guidance on the various types of documentation involved in the performance of a PRA. The project should realize that these technical reports on progress status eventually will become the primary sources of material for the final report. Effort involved in producing these reports should not be wasted, and QA procedures for documentation should be put into place to assure that these intermediate deliverables are effectively utilized.

A process for documentation quality assurance is one that ensures that the intent of each form of PRA documentation, as described in Chapter 3, is achieved and that the information is placed into a format and structure that eases the process of verification, if warranted.

Quality assurance measures should be instituted to ensure that technical reports contain aids for clearly backtracking the results to various risk measure levels, e.g., core damage frequency, system unavailability, or component unreliability. Documentation describing the methodology should be structured to facilitate separation (or partitioning) of the results into specific and identifiable contributors of risk. The documentation QA process should also have checks for assuring that the limitations and key assumptions at each major step in the execution of the PRA are clearly stated, especially with respect to the issues of completeness and uncertainty. Documentation also must be complete to the extent that the study is traceable and the results are reproducible, both during the course of the study and afterwards. The organization and scope of the final report(s) should convey the qualified results and should present information in a manner that is relevant to, understandable by, and compatible with the needs of the end user or users: PRA practitioners, plant managers, plant operators, regulators, and others.

4.2.6 QA Programs

A review process can be considered as an element of QA employed to verify accuracy, to assure completeness, and to help provide credibility of the PRA results, models, and conclusions. Reviews are an important technical element of the PRA process. A well-organized and structured review process is needed to improve confidence in the decisionmaker as to the usefulness of the PRA as a tool for managing the design, operation, and regulation of the facility against normal (highly probable) and abnormal (highly improbable) events. To ensure quality, past PRA studies have employed QA programs that involve four types of reviews. These can be classified (EPRI, 1983) as:

- Internal Intradisciplinary: type of review performed within a task by other study team members working on the task, including plant/utility personnel.
- Internal Interdisciplinary: type of review in which reviewers are part of the PRA study team, covering quality concerns that extend beyond the scope of individual tasks.

- External Technical: type of review conducted by PRA practitioners who are close to the working levels but outside the PRA study team.

- External Oversight: type of review conducted by recognized high-level experts who are outside the PRA study team.

Guidance in the conduct of peer reviews can be found in the open literature (see references in Section 4.10). For this project, the discussions on the PRA review process are based on the steps delineated in IAEA (1990) and Parkinson et al. (1984).

In Parkinson et al. (1984), the review process addresses two levels of review: high-level and technical-level reviews. A high-level review should be structured to answer the following questions:

- Can the type and source of the input be expected to support the objectives of the PRA task(s) under review and thereby the conclusions of the study?

- Can the methods of analysis logically transform the input into results that can support the objectives of the PRA task(s) under review and, therefore, the conclusions of the study?

- Do the outputs (results) of the PRA task(s) under review seem reasonable?

Questions to be addressed at the technical-level review are:

- Has the specific input to the PRA task under review been adequately demonstrated to support the objectives of this task and, therefore, the study conclusions?

- Do the inherent limitations of the methods and/or the practical constraints encountered during task execution impact the results of the task under review and, therefore, the conclusions of the study?

- Were the results (the output of the task) calculated correctly?

From these sets of questions, general evaluation criteria for the review process can be established for each technical area of the PRA. A logical flow can be established by defining a set of review questions for each evaluation criterion. For example, generalized technical questions presented in Table 4-1 can be used as guidelines for developing specific questions for the *three basic parts* of each technical area: the *input* data required by the task, the *method(s)* used to meet the task objectives, and the adequacy of the task *output* (the results) for providing input to the next sequential task or for meeting the overall objectives of the program.

The specific PRA technical areas that should be covered in the review of a Level 1 PRA include:

- Initiating event identification and grouping
- Accident sequence (event tree) analysis
- System (fault tree) analysis
- Analysis of dependent failures
- Human reliability analysis
- Database development
- Accident sequence quantification
- Uncertainty analysis
- External event analysis
- Display and interpretation of results.

For each of these technical areas, the review team should develop detailed questions that will help guide the reviewer to important issues that require information collection, review preparation, review implementation, and documentation. The tables in Appendix A present examples of the types of questions review teams might ask for each of the preceding technical areas[1]. The emphasis of the review depends on the product undergoing the review. Some of these review factors are highlighted in the following text.

Review of the initiating event activity should focus on how well plant information has been integrated, the selection and grouping of initiating events, and the identification of and success for

[1]In a similar manner to the Level 1 PRA quality assurance discussed here, technical areas with associated questions are needed for Level 2 and Level 3 PRA quality assurance.

Table 4-1 Generalized questions

High-Level Review	Technical-Level Review
INPUT	
• What input is required? • What is the source of the input? • How is the source of the input characterized? – generated by other tasks – taken from plant design and environs description – inferred from operating history – determined by assumption – taken from experimental results – taken from analytical results – other	• To what specific input are the objectives sensitive? • What are the important input data? (If appropriate, what are the specific values of that data?) • What is the specific source of each? (e.g., what experimental results?) • What is the nature of the uncertainty associated with the specific input? – applicability of sources to requirements (e.g., release from fuel data: small-mass experiments versus large-mass actual case) – variability (e.g., manufactured rebar strength varies even for the same grade) – lack of experience – uncertainty in the results of other analyses
METHODS	
• Is the methodology clearly outlined? • How are the methods characterized? – consistent with the project's procedures guide – confirmed by experiment (or otherwise validated or verified) – new (to PRA) – other	• What are the inherent limitations? • What modeling assumptions are made? • How is the uncertainty in the methods characterized? – completeness (inclusion of relevant factors) – accuracy (correct depiction of the logical relationships between the factors) • What is the impact of the uncertainties associated with the results of this task? • What is done to reduce the uncertainties associated with the model completeness or accuracy?
RESULTS	
• What is the nature of the results? • How do these results compare with the results of similar analyses?	• What are the specific results of this task? • To which specific results are the objectives of this task and, therefore, the (postulated) conclusions sensitive? • Reconstruct (in summary form) these specific important results.

frontline systems. Emphasis in the review of the event trees should be on the appropriateness of the event headings and on the proper representation of system and phenomenological dependencies in the event tree structure. Assumptions made in addressing phenomenological dependencies should be carefully documented and reviewed.

For the review of fault trees, particular attention should be given to the top logic of the fault tree, fault tree termination, and the consistency of system-specific assumptions applied to identify basic events, especially for similar components. Review of the human reliability task should ensure that test, maintenance, and emergency procedures have been thoroughly reviewed for potential sources of human error. Assumptions associated with the human reliability analysis of accident response errors should be reviewed, particularly by plant personnel, to ensure that the scenarios analyzed reflect expected accident conditions in terms of timing, information, and actions to be performed.

Much of the activity associated with accident sequence quantification involves computer-generated output, making the review of this PRA element difficult. Software QA procedures that should be in place will help allay some of the concerns on quantification. The cutsets in dominant accident sequences should be reviewed to ensure that they actually will cause the sequence to occur and that recovery factors are plausible and will reflect an understanding of the actions to be taken in these sequences. Review of major milestone reports should ensure that conclusions (findings) are clearly stated and the assumptions employed in the methodology are unambiguous and relevant information is provided so that audit checks can be made.

More guidance on review elements can be found in the noted tables. These tables are based on Parkinson et al. (1984) and are reproduced here with additions and modifications as a guide for the PRA project team, not only for anticipating the areas an external peer review team may focus on but also to emphasize the issues that will have to be addressed during intradisciplinary reviews by task team members. In preparation of external reviews, internal procedures should be set up so that the analysts for each technical area can present and defend their work to their associates while covering the issues delineated in these tables. These sets of questions also can guide the PRA project manager in developing QA procedures that will aid in assuring that the technical work is complete, accurate, and consistent, and that the results are verifiable.

4.2.7 Development of QA Programs

The planning and management task of a risk study is not only concerned with the definition of program objectives, the selection of the study team, methods, and the formulation of the project plan, it is also concerned with the definition and development of a QA plan for the PRA project. Part of the QA program should also include a review of the programmatic elements of the project and the technical elements listed above.

The project should develop and implement a QA plan, having as a minimum procedures for the following QA activities:

- document control
- independent technical reviews
- software quality assurance
- personnel QA training.

Examples of procedures for some of these QA activities are provided in Appendix B. These were extracted from approved and working QA plans. They are included in this document as exhibits of some select elements of a QA plan, which were developed to be compatible within a given organizational structure. As such, the QA protocol presented in these examples may not fit within the boundary of this PRA project. Hence, they should only be used to provide some guidance in the formulation of the project's QA plan.

4.3 Products

The major product from this task is a QA plan that has the attributes described in the previous sections.

4.4 References

EPRI, "An Approach to the Assurance of the Technical Adequacy in Probabilistic Risk Assessment of Light Water Reactors," EPRI-NP-3298, Electric Power Research Institute, 1983.

Garrick, B. J., "Considerations in the Achievement of Quality in Probabilistic Risk Assessment," UCLA-ENG-8269, University of California at Los Angeles, 1984.

IAEA, "Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1)," IAEA Safety Series No. 50-P4, International Atomic Energy Agency, 1992.

IAEA, "Procedures for Conducting Independent Peer Reviews of Probabilistic Safety Assessments," IAEA-TECDOC-543, International Atomic Energy Agency, 1990.

Parkinson, W. J., et al., "An Intensive Peer Review for Probabilistic Risk Assessment," NSAC-67, Electric Power Research Institute, March 1984.

PART B - PRA SCOPE

5. PRA SCOPE

The objective of this task is to define the scope of the probabilistic risk assessment (PRA). Figure 1.1 illustrates the five components that define the scope of the PRA. Figure 5.1 shows the important relationships between the five components of this task and the other major tasks of the PRA. These relationships are discussed below in Section 5.1.

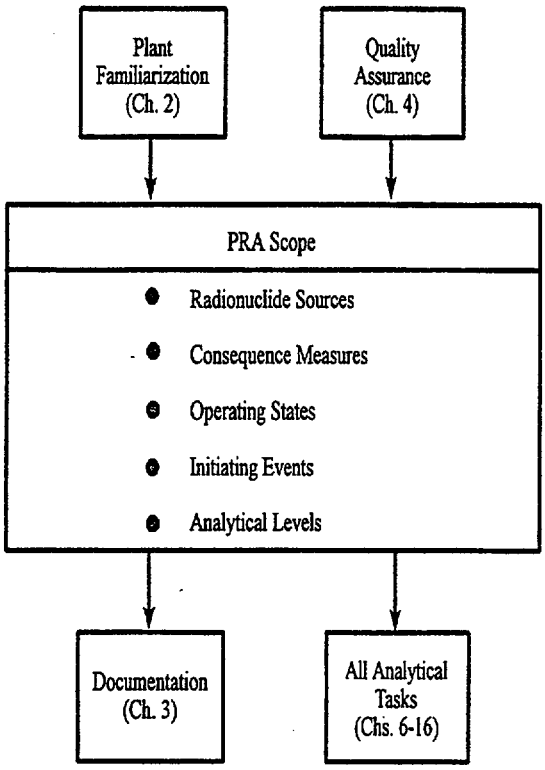


Figure 5.1 Relationships between PRA scope and other tasks

5.1 Relation to Other Tasks

As identified in Figure 5.1, the current task defines the scope of the analytical tasks needed for the PRA. In addition, the task provides basic information on the final documentation required. The figure also indicates the importance of applying the principles of quality assurance in this task and that information is needed from the Plant Familiarization task (Chapter 2).

5.2 Task Activities

The five components illustrated in Figure 5.1 define the scope of the PRA. It is first necessary to identify all potential sources of radioactivity and decide on how many of these sources will be included in the PRA. It is also necessary to determine the spectrum of consequence measures to be considered (e.g., health effects to the plant personnel or the surrounding population). Accidents can occur while the plant is at full power, low power, or during a shutdown condition. The plant operating states to be considered in the PRA should, therefore, be clearly identified. The type of possible events that can initiate an accident also needs to be defined. Initiating events internal to the plant usually include transients, loss-of-coolant accidents, fires, and floods. A complete PRA involves three sequential analytical parts or "levels" as shown in Figure 1.1. The three analytical levels are defined in Chapter 1. The number of levels needed for a particular PRA depends upon the end use.

Each of the five components are discussed in more detail below.

5.2.1 Radionuclide Sources

This component defines the starting point of the risk assessment by identifying plant hazards and characterizing the radioactive sources at the plant site. In general, the range of hazards that should be considered will depend on the scope and proposed end use of the PRA (i.e., worker risks, risks to the general public, and/or societal risks). Even if the assessment of worker risk is not a requirement, possible acute effects of radioactive and chemical hazards on the workers and their performance can have a significant impact on the evolution of the accident scenario and on the likely progression of plant damage, such as core damage.

Typically, there are several sources of radioactive material at a plant site. These include the irradiated fuel in the vessel, the spent fuel and spent fuel storage facilities, gaseous and liquid waste tanks and facilities, and perhaps other sources such as those used for calibration and diagnostic purposes. The exact radionuclide inventory of each of these sources is not likely to be known precisely and indeed the inventories can vary in time. However, useful bounds on these inventories can be expressed based on conservative evaluations or design limits.

Presently, the scope of the Kalinin PRA is to determine the frequency of core damage resulting from postulated upset conditions during full power

operations. For the purpose of this PRA, the amount of radioactive nuclide material in the reactor core is conservatively assumed to correspond to the end of core life (i.e., immediately before refueling). This assumption would not only characterize the inventory of the reactor core for the purposes of assessing the potential hazards, but it would also define the level of decay heat. The amount of decay heat assumed to be present at the onset of each potential accident scenario directly influences the determination of the criteria for classifying the success of engineered safety systems designed to mitigate the progression of the postulated accident and operator performance under emergency conditions.

5.2.2 Consequence Measures

As noted above, it is necessary to determine the spectrum of consequence measures to be considered in the PRA. The focus in past PRAs has been on calculating the core damage frequency (CDF) and the contribution of various accident sequences to the total CDF. In order to calculate the CDF, a Level 1 PRA is needed. A Level 1 PRA is useful for determining what combination of system failures and operator actions contribute to the predicted CDF. This can be used to identify preventative measures for lowering the CDF at a plant.

Another important consequence measure calculated in past PRAs is offsite health effects. A Level 3 PRA is needed to calculate offsite consequences. As noted above, onsite consequences to plant personnel are usually not included in a Level 3 PRA.

The scope of these procedure guides includes all three analytical levels (i.e., a Level 3 PRA).

5.2.3 Operating States

This component delineates the plant operating states that potentially can contribute to the overall risk profile. PRAs have often considered only one plant operating state (i.e., full power operation) in which an accident may be initiated. There are, however, other plant operating modes (see Table 5-1) in which other accident initiators might occur and the assessment of risk may be warranted. In these cases, the success criteria and the unavailability of some systems might differ from those for full power operation. Examples of studies that focused on other plant operating modes are described in Bley et al. (1985); Moody et al. (1988); Whitehead et al. (1994), Chu et al. (1994); and PLG (1994).

Table 5-1 Plant operating states

• Nominal full power operation
• Reduced power operation
• Reactor critical, turbine not operating
• Reactor subcritical, reactor coolant system pressure above the maximum pressure for residual heat removal conditions
• Reactor subcritical, low pressure residual heat removal systems in operation
• Reactor subcritical, main circuit open (for example, for refueling, steam generator maintenance, or reactor coolant pump maintenance)

From a practical point of view, conducting the PRA for full power operation can be considered a first step in a comprehensive risk analysis program. The consideration of other plant operating states is important in order to understand the complete risk profile of the plant. Exclusion of any operating state(s) of the plant from the PRA should be justified. The justification may be based on the scope of the safety assessment or on some resource constraint. The justification may also be based on a judgment that for certain operating states the contribution to the overall risk would be small.

The current scope of the Kalinin PRA is to determine the plant's risk profile for a set of

initiating events postulated to occur during full power operation of the plant. At a later date, other plant operating states may be considered. Most PRAs performed for U.S. plants assumed that a single plant model adequately captures the plant configuration during full power operation. This may not be the case for the Kalinin plant. It may be necessary to develop a number of plant models to represent adequately the Kalinin plant in all possible full power configurations. The Kalinin Nuclear Power Station's maintenance and operating practice must be reviewed to determine off-normal system lineups and maintenance configurations. All configurations that affect the reactor coolant system or systems that contribute to risk should be described and the time in each configuration determined. Special initiating events for each configuration, unique event sequences, and system unavailabilities may exist. These should also be identified.

5.2.4 Initiating Events

Initiating events are broadly categorized into two categories: internal initiating events and external initiating events. Internal initiating events are system and equipment malfunctions (e.g., those leading to plant transients or pipe breaks) inside the plant. Analyzed along with internal initiating events is the loss-of-offsite electrical power.

External events are usually categorized into two classes depending upon the location of the hazard. One class of hazards is clearly related to the plant site, its location, or its surrounding environment. Specific examples of external events from this class include external flooding, high winds, seismic activity, and ice storms. Note that many of these external events can cause a loss-of-offsite power in addition to other adverse impacts on the plant.

The second class of hazards originates from vulnerabilities within the plant. Examples of this class of external events include fires, internal flooding, caustic chemical releases, explosions, and missiles from rotating equipment. Identification and characterization of the hazards associated with this second class of events is addressed in the spatial interactions analysis (Section 8.3). Although internal flooding and fire events are conventionally treated in PRA studies as external events, they are included in the internal event category in this PRA. Evaluation of sabotage events is not currently included as part of the scope of a PRA.

A screening approach is used to identify external hazards particular to the site and its environment that may warrant further consideration. The starting point is a comprehensive list of natural and man-made external events, such as that shown in Table 5-2, which was adopted from NRC (1983). Each hazard is screened in order to select those that are considered significant for detailed analysis. Besides the events listed in Table 5-2, other sources of information that should be reviewed to identify other potential hazard sources include: safety analysis reports pertaining to the site characteristics and regional growth plans (including future projections in industrial activities, such as roads, pipelines, and air traffic).

Events that do not meet the following criteria would normally be retained for further analysis in a PRA. (These criteria are used in Table 5-2.)

1. The event is of equal or lesser damage potential than the events for which the plant has been designed.

2. The event has a significantly lower frequency of occurrence than other events with similar consequences.

3. The event cannot occur close enough to the plant to affect it.

4. The event is included in the definition of another event.

For those events that are retained, the full spectrum of hazard severity must be considered. Often this is facilitated by subdividing the hazard severity range and analyzing each element separately.

The scope of the Kalinin PRA currently includes consideration only of internal initiating events, internal fires, internal floods, and seismic events. Guidance for the treatment of seismic events is found in Chapter 14. Presently, no other external events associated with the site, its location, or its environment are included in the Kalinin PRA.

Table 5-2 Natural and man-induced external events to be considered in a PRA (NRC, 1983)

Event	Relevant Screening Criteria	Remarks
Aircraft impact	----	Site specific, requires analysis
Avalanche	3	Site selection criteria should preclude
Biofouling	--	Site specific, may require analysis
Coastal erosion	4	Should be considered in analysis of external flooding
Drought	4	Should be considered in analysis of loss of heat sink
External flooding	---	Site specific, requires analysis
Extreme winds and tornadoes	--	Site specific, requires analysis
Fog	1	Could influence transportation/industrial accidents
Forest and external fires	---	Site specific, requires analysis
Frost	1	Snow and ice dominate
Hail	1	Other sources of missiles more severe
High summer temperatures	4	Should be considered in analysis of loss of heat sink
High tide, high lake level, or high river stage	4	Should be included in analysis of external flooding
Hurricane	---	Site specific, may require analysis
Ice cover	4	Should be considered in analysis of loss of heat sink
Ice storm	---	Site specific, may require analysis
Industrial or military activities	---	Site specific, may require analysis
Landslide	3	Site selection criteria should preclude
Lightning	1	Typically included in plant design
Low lake or river water level	4	Should be considered in analysis of loss of heat sink; may involve consideration of degradation of water quality
Low winter temperature	1	Typically included in plant design
Meteorite	2	Typically small frequency

Table 5-2 Natural and man-induced external events to be considered in a PRA (NRC, 1983) (Cont'd)

Event	Relevant Screening Criteria	Remarks
Microbe induced corrosion	---	Site specific, may require analysis
Pipeline accident (toxic material, flammable material or high pressure)	---	Site specific, may require analysis
(Intense) precipitation	4	Should be included in external flooding analysis
River diversion	4	Should be considered in analysis of loss of heat sink
Sandstorm	1	Typically considered in design, if appropriate
Seiche	4	Should be included in external flooding analysis, if appropriate
Seismic activity	---	Site specific, requires analysis
Sinkhole	1	Should be considered in plant design
Snow	1	Should be considered in plant design
Soil shrink-swell consolidation	1	Should be considered in plant design
Storm surge	4	Should be included in external flooding analysis, if appropriate
Toxic gas	---	Site specific, may require analysis
Transportation accidents	---	Site specific, requires analysis
Tsunami	4	Included in seismic and external flooding analysis, if appropriate
Missiles from high energy equipment	---	Site specific, requires analysis
Volcanic activity	3	Siting should preclude
Waves	4	Included in external flooding analysis

5.2.5 Analytical Levels

The three analytical levels of a PRA are defined below:

- Level 1 - involves the identification and quantification of the sequences of events leading to core damage;
- Level 2 - involves the evaluation and quantification of the mechanisms, amounts, and probabilities of subsequent radioactive material releases from the containment; and
- Level 3 - involves the evaluation and quantification of the resulting consequences to both the public and the environment. Consequences to plant personnel are usually not included in a Level 3 PRA.

The PRA level needed depends upon the consequence measures to be calculated (refer to Section 5.2.2 above). Presently, the scope of the Kalinin PRA includes all three analytical levels.

5.3 Products

The major product from this task is a definition of the scope of the PRA.

- Radionuclide Sources
  - The product of this activity is a characterization of the radioactive sources, which are to be included in the PRA, at the plant site.
- Consequence Measures
  - The product of this activity is a description of the consequence measures to be calculated in the PRA. The selection of consequence measures determines the analytical level needed in the PRA.
- Operating States
  - The product of this activity is a listing of the plant operating states to be included in the PRA.
- Initiating Events
  - The product of this activity is a listing of all initiating events (internal or external to the plant) that are to be included in the PRA.
- Analytical Levels
  - The product of this activity is a determination of how many analytical levels will be calculated in the PRA.

5.4 References

Bley, D. C., et al., "Zion Nuclear Plant Residual Heat Removal PRA," NSAC-84, Electric Power Research Institute, July 1985.

Chu, T.-L., et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown at Surry, Unit 1," NUREG/CR-6144, Brookhaven National Laboratory, June 1994.

Moody, J. H., et al, "Seabrook Station Probabilistic Safety Study - Shutdown Modes 4, 5, and 6," New Hampshire Yankee, May 1988.

NRC, "PRA Procedures Guide," Chapter 10, NUREG/CR-2300, U.S. Nuclear Regulatory Commission, January 1983.

PLG, "Gösgen Probabilistic Safety Assessment - Module IV, Event Sequence Models for Nonfull-Power Modes," prepared for Kernkraftwerk Gösgen-Däniken AG, PLG-0870, PLG, Inc., February 1994.

Whitehead, D., et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1," NUREG/CR-6143, Sandia National Laboratories, 1994.

PART C - LEVEL 1 GUIDELINES

6. INITIATING EVENT ANALYSIS

The objective of this task is to develop a complete list of initiating events grouped into categories that would facilitate further analyses. An initiating event is an event that creates a disturbance in the plant and has the potential to lead to core damage, depending on the operation of the various safety systems as well as the response of the plant operators. The initiating event analysis is the first task of the first element of a Level 1 probabilistic risk assessment (PRA) (refer to Figure 1.3). The initiating event analysis consists of identification and selection of events and grouping of these events. Figure 6.1 shows the important relationships between this task and the other major components of the PRA. These relationships are discussed in Section 6.1.

6.1 Relation to Other Tasks

As indicated in Figure 6.1, this task has extensive interactions with the following other PRA tasks:

Plant Familiarization. In this task, plant systems and major components (including operating instructions) are reviewed to determine whether any of the failure modes could lead directly to core damage. Special attention is given to identifying common-cause initiators.

Quality Assurance and Documentation. This task has obvious interfaces with QA requirements and provides input to the PRA documentation.

PRA Scope. Work beyond the full power operating state is not currently in the scope for the Kalinin PRA. For studies that consider additional states, new initiating events may need to be considered.

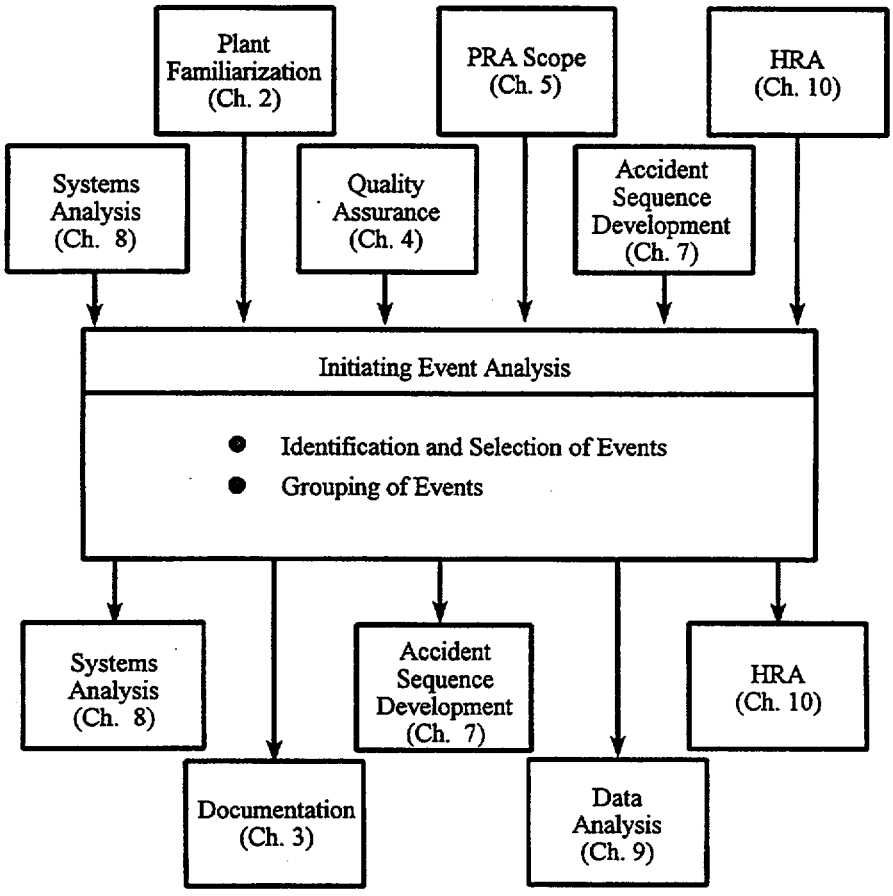


Figure 6.1 Relationship between initiating event analysis and other tasks

Accident Sequence Development. The accident initiators provide the starting point for the accident sequence development, and the dependencies between initiators and system response are crucial to sequence development and quantification.

Systems Analysis. In this task, support system failures which can cause initiating events are identified. The initiating events task also provides important information to the systems analysis task as to how systems performance is impacted by a particular initiator.

Data Analysis. This task provides the information needed for the quantification of the initiating event frequencies.

Human Reliability Analysis (HRA). The HRA could influence or modify the identification and selection of initiating events. More importantly, the HRA will influence the grouping of initiating events.

Fire Analysis. Fires can induce multiple internal initiating events and affect multiple systems helpful for recovery; therefore, revisions to the event tree structures and definitions of top events may be required.

Flood Analysis. Floods can induce multiple internal initiating events and affect multiple systems helpful for recovery; therefore, revisions to the event tree structures and definitions of top events may be required.

Seismic Analysis. Earthquakes can cause simultaneous failures in structures and equipment needed to prevent core damage. These common-cause failures can require significant revisions or additions to internal event PRA models.

6.2 Task Activities

The initiating event analysis consists of two activities: (1) identification and selection of events and (2) grouping of events. These activities are described below in general terms. An early reference, in which detailed guidance for performing these activities can be found, is NRC (1983). A more recent discussion can also be found in NRC (1997). In addition, it is also useful to refer to lists of initiating events used in previous PRAs. Such references are provided in Section 6.2.2.2.

Prior to describing the two activities, important assumptions and limitations are provided.

6.2.1 Assumptions and Limitations

The present task classifies initiators as either "internal" or "external." Internal initiators are plant upsets that are associated with the malfunction of plant systems, electrical distribution systems, or are a result of operator errors. External initiators originate outside the plant. They are due to hazards, such as external fires and floods, seismic activity (refer to Chapter 14), or other environmental stresses. Fires (refer to Chapter 12) and floods (refer to Chapter 13) that occur internal to the plant are conventionally treated in PRA studies as external events; however, they are included in the internal event category in this PRA.

The initiating events used in a PRA are by no means confined to those postulated for design and licensing purposes nor are they associated with qualitative qualifiers, such as "credible" or "anticipated." Identification of initiating events also requires a new way of thinking for design engineers, operators, and regulators, i.e., one focused on the propagation of plant failures. Review of previous analyses and operational events can help develop the desired viewpoint. Departures from design, through material substitution or field modifications during construction, must be considered in the identification of initiating events.

Once the set of initiators has been finalized, any other initiators that could have been included are either presumed to contribute little to the overall risk or are considered outside the present scope of the project. For the Kalinin PRA, the only "external" events that are considered in the present scope are: seismic, internal fires, and internal floods.

The disposition of low frequency initiating events should be documented. For example, in some PRAs, major structural failure of the pressure vessel is not explicitly represented since it is argued to be such a low frequency event which

does not contribute significantly to the risk. In other PRAs, this event has been quantitatively considered by designating it to a specific initiator category, "excessive LOCA," to describe loss-of-coolant accidents that are beyond the capability of core reflooding and cooling capabilities.

In general, the impact of all possible plant operating states on the physics and operational considerations leading to specific initiating events should be considered. However, under the present scope of the Kalinin PRA, the only plant operating state to be considered is full power operation.

It should also be recognized that it is not possible to fully ascertain the completeness of any list of initiators. The initial list of initiators that pertains specifically to the plant being analyzed is presumed to be as complete as possible. The PRA analysis may subsequently reveal additional initiating events, particularly as subtle interactions involving support systems are more completely understood by the PRA analysts. Accordingly, the initial grouping of initiators from this task may require modification as the PRA proceeds.

6.2.2 Identification and Selection of Events

There are several ways for identifying internal initiating events, each having its strengths and limitations. Since the aim is to produce an initiating event list that is as complete as possible, it is recommended that all approaches should be followed in parallel, although one approach may be selected as the main approach. These approaches usually complement each other, especially if they are performed together. The following lists four ways that internal initiating events can be identified:

1. Engineering evaluation
2. Reference to previous initiating event lists
3. Deductive analysis
4. Operational experience.

As described below, these four approaches complement each other providing reasonable assurance that the list of initiating events is as complete as possible.

6.2.2.1 Engineering Evaluation

In this approach, the plant systems (operational and safety) and major components are systematically reviewed to determine whether any of the failure modes (e.g., failure to operate, spurious operation, breach, disruption, collapse) could lead directly, or in combination with other failures, to core damage. Partial failures of systems should also be considered. These types of failures are generally less severe than a complete failure, but they may be of higher frequency and are often less readily detected.

Special attention should be given to common-cause initiators, such as the failure of support systems (e.g., specific electric power buses, service water, instrument or control air, or room cooling features). Postulated failures are sought that result in (or require) the plant or turbine to trip (or runback) and can cause additional systems to fail. Reviews of plant and system operating instructions and abnormal operating instructions of Western plants have been found useful for identifying subtle interactions between systems. The experience acquired in these investigations should be utilized here as well.

Tables 6-1 and 6-2 give examples how failures of support systems and "abnormal operating instructions" (AOIs) could be scrutinized and evaluated as part of an effort to identify potential initiating events.

6.2.2.2 Reference to Previous Initiating Event Lists

It is useful to refer to lists of initiating events drawn up for previous PRAs on similar plants and from the safety analysis report. This may, in fact, be the starting point. IAEA (1993a) and INEL (1985), for example, provide lists of initiators used in selected light water reactor full power PRAs. Chu et al. (1994) and PLG (1985) provide examples for pressurized water reactor shutdown PRAs. IAEA (1994) is of particular interest since it deals directly with identifying and grouping PRA initiating events for VVER reactors at full power PRAs. Table 6-3, taken from IAEA (1994), provides a list of generic initiators for VVER-1000 plants. Note that Table 6-3 lists some external

initiators as well as a reasonably comprehensive list of internal initiators. IAEA 1992) and IAEA (1993b) are additional useful sources of information for review.

Table 6-1 Format for failure modes and effects analysis of key support systems

System/ Subsystem	Failure Mode	Effect	Initiating Event Category	Plant Model Designator	Comments
All systems or subsystems under consideration are identified; for example, the standby diesel generator fuel oil supply	The faults or failure modes identified as part of the failure modes and effects analysis are described; for example, a fault leading to inadequate fuel oil to standby diesels	The impact of the faults on the plant response are described; for example, loss of standby diesel generator power source	The initiating event categories impacted by the failures are identified	The plant models affected by the failures are identified	Any remarks that would clarify the failure modes and their impact on the plant models should be added

Table 6-2 Format for abnormal operating instruction review summary

AOI Reviewed	Potential Initiating Event Category	Initiating Event Category	Plant Model Designator	Comments
All operating instructions that are evaluated should be identified	The initiating event categories affected should be identified against the corresponding AOIs	The initiating event categories impacted by the AOIs are identified	The plant models affected by the AOIs are identified	Any remarks that would clarify the AOIs and their impact on the plant models should be added

Table 6-3 Generic list of initiating events for VVER-1000 reactors (IAEA, 1994)

General Categories	Initiating Events
General Plant Transients	•Trip of one of two; two of three; or two of four main coolant pumps •Main coolant pump seizure •Total loss of primary coolant system flow/trip of all main coolant pumps •Feedwater flow reduction due to control malfunctions or loss of flow path •Excess feedwater •Inadvertent closure of main steam isolation valve •Inadvertent closure of turbine stop valve •Turbine control valve malfunction •Turbine trip •Total loss of load[1] •Generator fault[1] •Loss of one 6 kV bus bar •Loss of substation switchyard or unit transformer •Loss of intermediate cooling to main coolant pumps •Spurious reactor trip[2] •Reactor scram due to small disturbance[2] •Uncontrollable withdrawal of control rod •Uncontrollable withdrawal of control rod group •Inadvertent boron dilution •Control rod ejection without reactor vessel damage
Administrative Shutdowns	•Failure of pressurizer spray •Failure of pressurizer heaters •Loss of one feedwater pump •Minor miscellaneous leakage in feedwater/condensate system •Loss of a condensate pump •Inadvertent bypass to condenser •Administratively caused shutdown •Control rod/control rod group drop •Very small LOCA and leaks requiring orderly shutdown

[1]May lead to loss of secondary heat sink if loss of condenser vacuum occurs.

[2]Unavailability of reactor shutdown function is 0.0 (because reactor is tripped)

Table 6-3 Generic list of initiating events for VVER-1000 reactors (IAEA, 1994) (cont'd)

General Categories	Initiating Events
Loss of Secondary Heat Removal	•Loss of both feedwater pumps •Feedwater collector rupture •Feedwater line rupture that can be isolated by separation of one steam generator and compensated by reserve feedwater pump •Feedwater line rupture that can be isolated by separation of one steam generator and cannot be compensated by reserve feedwater pump •Rupture of feedwater pump suction line •Loss of several condensate pumps •Loss of condenser vacuum •Loss of circulating water
Loss-of-Offsite Power	•Loss of grid •Loss of all 6 kV busbars •Failure of unit auxiliary transformer
Non-Isolatable Steam/Feedwater Line Leaks Inside Containment	•Rupture of feedwater pump discharge line inside containment •Steam line rupture inside containment
Non-Isolatable Steam/Feedwater Line Leaks Outside Containment	•Rupture of feedwater pump discharge line outside containment •Inadvertent opening of steam generator safety valve •Inadvertent opening of atmospheric steam dump valve •Steam line rupture outside containment between steam generator and isolating valve
Isolatable Steam Leaks	•Rupture of main steam collector
Loss-of-Coolant Accidents (LOCAs) Inside Containment	•Reactor pressure vessel rupture •Large LOCA •Medium LOCA •Small LOCA •Small reactor coolant system leakage •Main coolant pump seal leakage •Control rod ejection and LOCA •Pressurizer power-operated relief valve leakage
LOCA Outside Containment	•Instrumentation/sample tube rupture •Leakage from make-up/letdown system •Leakage from residual heat removal system •Leakage through intermediate cooling system of main coolant pumps

Table 6-3 Generic list of initiating events for VVER-1000 reactors (IAEA, 1994) (cont'd)

General Categories	Initiating Events
Special Initiators (These need to be considered on a plant-specific basis and may lead to events already considered or a very complicated event requiring a failure modes and effects analysis.)	•Loss of noninterruptible AC power busbar •380 V bus failure •Failures in essential DC system •Failures in essential AC power system •Loss of power to protection/control system •Loss of service water system •Loss of intermediate cooling to main coolant pumps •Loss of high pressure air •Loss of room cooling in a vital instrumentation compartment •Loss of room cooling in a normal control system compartment •Spurious actuation of fire suppression systems (sprinkler + CO_2 + other) •Internal flooding (including spurious actuation of sprinkler system or fire extinguisher) •Internal fires •Flying objects including turbine •Hydrogen explosions in generator and gas blowdown systems

6.2.2.3 Deductive Analysis

In this approach, core damage is usually the top event in a "master logic diagram." To provide order to the master logic diagram, a hierarchical structure is employed. Each level of the structure is a result of events that categorize the level immediately below. The top event is, therefore, successively broken down into all possible categories of events that could cause the event to occur. Successful operation of safety systems and other preventive actions are not included. The events at the most fundamental level are then candidates for inclusion in the list of initiating events for the plant. An example of such a diagram is given in Figure 6.2 from PLG (1983). Eight hierarchical levels are depicted in the figure, with core damage at Level III. The intended use of this figure had been a bit broader than the objectives of this task.

The master logic diagram is a logic tree that identifies necessary conditions for occurrence of the top event, i.e., the top event can occur "only if" the lower level events occur. It is used to search for initiating events. Generally, additional events defined by an event tree must also occur before core damage is certain. (Note that the fault trees used in systems analysis are different logic models. They identify both necessary and sufficient conditions for failure of the top event, i.e., the top event is guaranteed to occur "if and only if" the logic of the tree is actualized.)

This example traces and documents the thought process that results from consideration of the question "How can a significant release of radioactive material to the environment around the site occur?" This question is represented by the box on Level I of Figure 6.2. Level II represents the argument that such a release must be from either a damaged core or a noncore source. (This argument was valid for the plant for which the example master logic diagram was developed.) Level III represents the argument that a significant release of radioactive material is possible only if excessive core damage occurs and the material escapes to the environment.

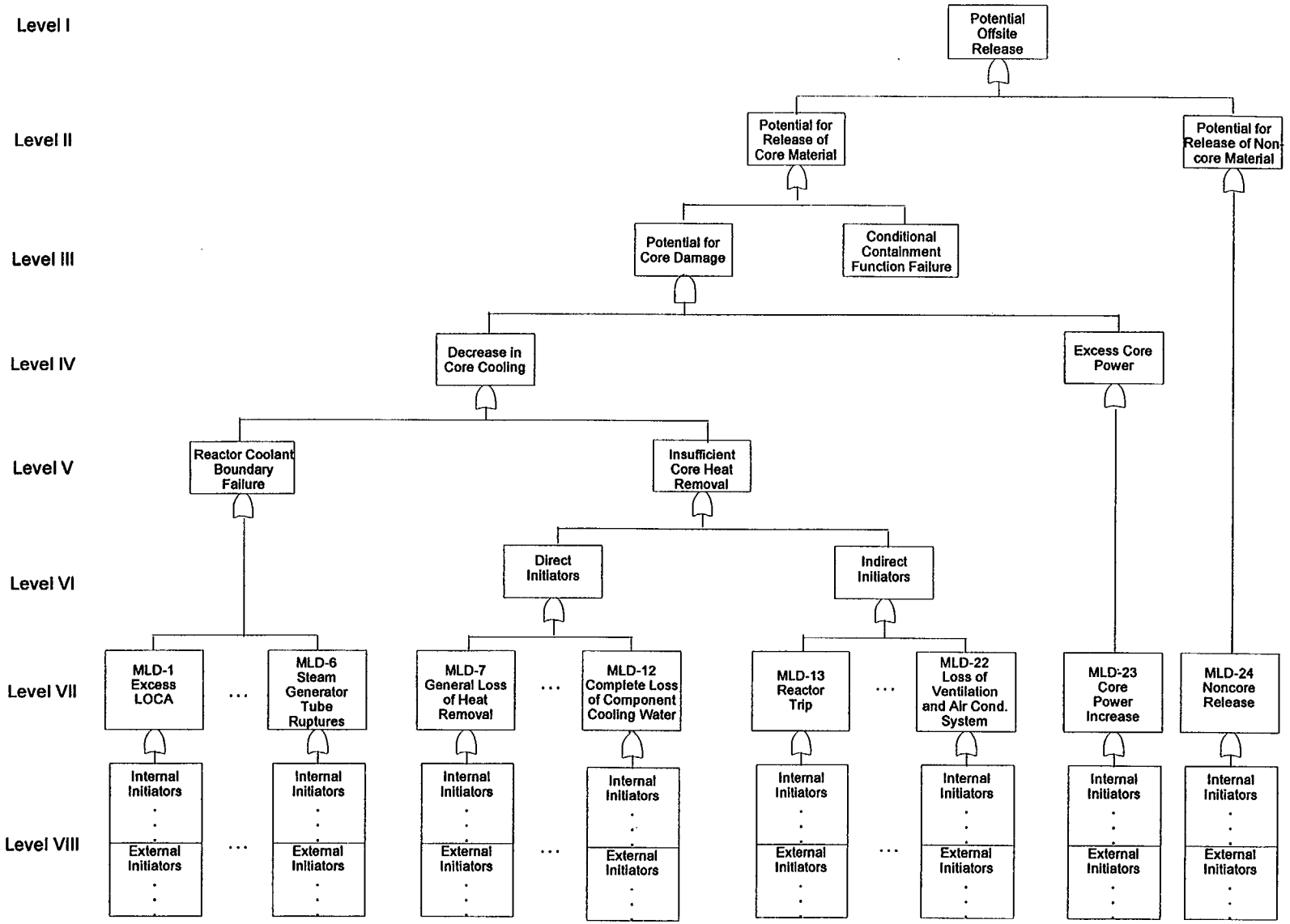


Figure 6.2 Master logic diagram

The remainder of the diagram emphasizes potential contributors to core damage. Plant sequences that ultimately result in extensive core damage involve either insufficient cooling of the core or other uncorrected mismatches between generated power and heat removal. This argument is represented by Level IV of the master logic diagram. Level V further delineates the logic for the case of "loss of core cooling" identified in Level IV: loss of core cooling occurs only if the reactor coolant boundary fails or if there is insufficient core heat removal. Level VI presents the logic that insufficient core heat removal is the result of either direct initiators or indirect initiators. Indirect initiators are those disturbances that require additional plant failures to result in the indicated impact. Initiating event categories are articulated in Level VII; specific initiators are then listed in tables that support Level VIII.

6.2.2.4 Operational Experience

In this approach, the operational history of the plant (and of similar plants elsewhere) is reviewed for any events that are not included in the list of initiating events. This approach is not expected to reveal low frequency events but could identify common-cause initiating events. It should also verify that the observed events can be properly represented by the mitigating event categories being developed through exercise of the previous approaches. The list of initiating events should be reviewed for any inadvertent omissions and, as a further check, to remove any repetitions or overlaps.

6.2.3 Grouping of Events

Once the task of assessing the requirements of the plant systems has been completed, the identified initiating events should be grouped (or binned) in a manner that would simplify the ensuing analysis. Each initiating event group should be composed of events that essentially impose the same success criteria on plant systems. Similarly, special conditions, such as, for example, similar challenges to the operator, similar automatic plant responses, and equipment functionality, should also be factored into this grouping process. In the process of grouping, it will become clear that some categories of initiating events will need to be subdivided further. Dividing LOCAs by break size (and perhaps location) is a well known example, but other cases should be expected. Some examples are: steamline break by size, loss of flow by number of failed pumps, and spurious control rod withdrawal by number of rods or rate of reactivity addition. The subsequent analysis needed may be reduced by grouping together initiating events that evoke the same type of plant response but for which the frontline system success criteria are not identical. The success criteria applied to this group of events should then be the most restricting for any member of the group. The saving in effort required for analysis must be weighed against the conservatism that this grouping introduces. The following criteria should be used when grouping initiating events:

- Initiating events resulting in the same accident progression (i.e., requiring the same systems and operating actions for mitigation) can be grouped together. The success criteria for each system required for mitigation (e.g., the required number of pump trains) is the same for all initiators grouped together. In addition, all grouped initiators should have the same impact on the operability and performance of each mitigating system and the operator. Consideration can also be given to those accident progression attributes that could influence the subsequent Level 2 analysis (Chapter 15).

- In conformance with the criteria above, LOCAs can be grouped according to the size and location of the primary system breach. However, primary breaches that bypass the containment should be treated separately.

- Initiating events can be grouped with other initiating events with slightly different accident progression and success criteria if it can be shown that such treatment bounds the real core damage frequency and consequences that would result from the initiator. To avoid a distorted assessment of risk and to obtain valid insights, grouping of initiators with significantly different success criteria should be avoided. The grouping of initiators necessitates that the success criteria for the grouped initiators be the most stringent success criteria of all the individual events in the group. Note that in a sound baseline PRA,

low-frequency initiators are grouped with other relatively high-frequency initiators, rather than excluding them from further analysis.

6.3 Products

As identified in the task Documentation (Chapter 3), the current task will produce draft material for the final report. Specifically, the work products for this task are a draft portion of the "Initiating Event Analysis" appendix of the main report. In addition, this task will provide:

- A list or general description of the information sources that were used in the task.
- Specific information/records of events (plant specific, industry experience, "generic" data) used to identify the applicable initiating events.
- The initiating events considered including both the events retained for further examination and those that were eliminated, along with the supporting rationale.
- Any quantitative or qualitative evaluations or assumptions that were made in identifying, screening, or grouping of the initiating events as well as the bases for any assumptions and their impact on the final results.
- Documentation of the failure modes and effects analysis performed to identify support system initiators and the expected effects on the plant (especially on mitigating systems).
- Specific records of the grouping process including the success criteria for the final accident initiator groups.
- Documentation of findings of failure modes and effects analysis (or equivalent) performed on systems, structures, and components within the scope of the change but not modeled in the PRA, to assess their impact on the scope and frequency of initiators.

6.4 References

Chu, T.-L., et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown at Surry, Unit 1," NUREG/CR-6144, Brookhaven National Laboratory, June 1994.

IAEA, "Generic Initiating Events for PSA for VVER Reactors," IAEA-TECDOC-749, International Atomic Energy Agency, June 1994.

IAEA, "Defining Initiating Events for Purpose of Probabilistic Safety Assessment," IAEA-TECDOC-719, International Atomic Energy Agency, September 1993a.

IAEA, Proceedings of the Workshop Organized by the IAEA and held in Moscow, 1-5 February 1993, Working Material, IAEA-RER/9/005-2/93, International Atomic Energy Agency, February 1993b.

IAEA, Report of a Workshop Organized by the IAEA and held in Řež, Czechoslovakia, 3-7 February 1992, Working Material, IAEA-J4-005/1, International Atomic Energy Agency, February 1992.

INEL, "Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessments," NUREG/CR-3862, Idaho National Engineering Laboratory, May 1985.

NRC, "The Use of PRA in Risk-Informed Applications," NUREG-1602, Draft for Comment, June 1997.

NRC, "PRA Procedure Guides: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, Volumes 1 and 2, 1983.

PLG, "Zion Nuclear Plant Residual Heat Removal PRA," prepared for Nuclear Safety Analysis Center of the Electric Power Research Institute, NSAC-84, PLG, Inc., July 1985.

PLG, "Diablo Canyon Probabilistic Risk Assessment," PLG-0637, prepared for Pacific Gas and Electric Company, PLG, Inc., January 1983.

7. ACCIDENT SEQUENCE DEVELOPMENT

Accident sequence development is the second component of the first element in a Level 1 probabilistic risk assessment (PRA) (refer to Figure 1.3). Accident sequence development consists of three interrelated tasks--namely, core damage definition, functional analysis and system success criteria, and event sequence modeling. This is shown on the flowchart in Figure 7.1. The first of these tasks defines the plant conditions that correspond to core damage in a manner that allows sequence and system success criteria to be unambiguously defined. The objective of the second task is to identify the success criteria forplant systems and components. The objective of the task on event sequence modeling is to determine the range of possible plant and operator responses to a wide variety of upset conditions and to develop event trees for all initiating event categories that are defined in the task Initiating Event Analysis.

Figure 7.1 shows the important relationships between the tasks under accident sequence development and the other major components of the PRA. These relationships are explored in more detail in each of the sections describing the three tasks. Core damage definition is discussed in Section 7.1, functional analysis and system success criteria in Section 7.2, and event sequence modeling in Section 7.3.

7.1 Core Damage Definition

The objectives of this task are: (1) to define the plant conditions that correspond to core damage in a manner that allows sequence and system success criteria to be unambiguously defined and (2) to specify clearly the plant conditions that represent successful termination of postulated scenarios.

7.1.1 Relation to Other Tasks

The relationships between accident sequence development and other PRA tasks are shown in Figure 7.1. Most of these tasks interface with the development of system success criteria (refer to Section 7.2) and event sequence modeling (refer to Section 7.3). The conditions for core damage (discussed in this section) need to be translated into system failure states (refer to Section 7.2) for the purpose of establishing success criteria.

7.1.2 Task Activities

To meet the objectives of this task, it must be understood that the physical characteristic of the core that defines core damage has a strong influence on the magnitude of core damage frequency determined by the risk model (see Section 7.2, Functional Analysis and System Success Criteria). Excessively conservative definitions of core damage will yield higher assessed core damage frequencies and, more importantly, will likely impact the perception of the importance of the individual contributors to risk. Risk models that do not fully account for the robustness in the plant design also can contribute to higher damage frequencies.

A similar concern exists with specifying the conditions for successful termination of an accident scenario. Using overly conservative criteria (e.g., requiring all scenarios initiated at full power to proceed to cold shutdown for successful accident termination) could strongly influence the model structure and complicate the modeling requirements with little or no added understanding in the factors contributing to the risk.

Likely sources of conservatism are in the analytical tools (available analyses and computer codes) used in the determination of the outcome of postulated accident scenarios. The definition of core damage must be consistent with the available analytical tools.

If conservatisms built into the definition, criteria, plant models, and analyses are suspected to strongly influence the end result of an accident analysis calculation, then the result should be refined. This should be done selectively using more realistic models, but only after the relative importance of all the accident sequences have been initially assessed. It would then be possible to judge the importance of resolving whether a particular sequence of events could or could not lead to core damage, as initially predicted. This iterative nature of reevaluating the results brings with it a caution: sequence-specific refinement is not performed on sequences that are not "important" and, therefore, use of information from unimportant sequences must be made with caution. However, it does make use of time and resources more effectively by consistently focusing on the more important accident scenarios.

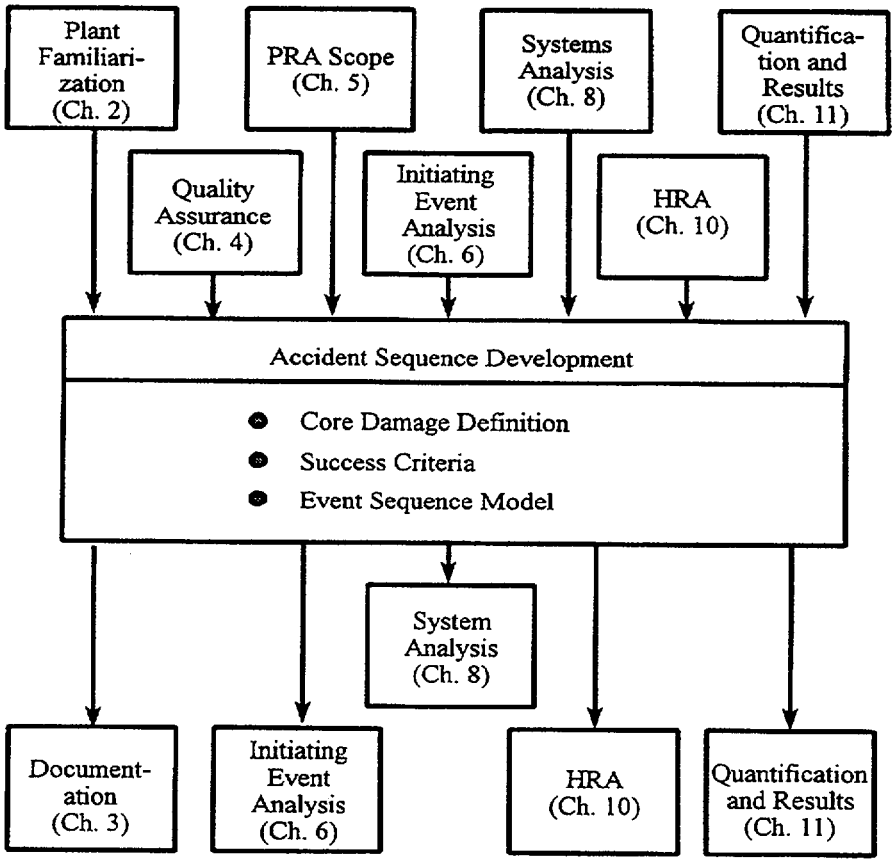


Figure 7.1 Relationships between accident sequence development and other tasks

The safety philosophy embedded in the reactor design, particularly with respect to design basis accidents, must be reflected in the definitions of "core damage" as well as "success." Impacts of design basis accidents on the public near the site boundaries, and on the operators and engineers within the site boundaries, need to be considered if the successful termination of such accidents has the potential to impact the plant personnel.

A Level 1 PRA usually entails identifying scenarios that lead to severe core damage and determining the corresponding accident scenario frequencies. The most important definition that must be made in this task is that of core damage.

There are several possible degrees of "core damage," the severity depending on the extent of core damage and on the magnitude of the resulting releases of radioactive material from the core. One definition of core damage is uncovery and heatup of the reactor core to the point where prolonged clad oxidation and severe fuel damage is anticipated.

Releases of radioactive material in scenarios that do not involve core damage could be of concern, also if these releases are sufficient to trigger emergency responses offsite. Minor radioactive releases may be from in-core sources or from radionuclides resident in the primary coolant

circuit. However, for the Kalinin PRA, core damage will define the scope of the study. The undesired end result of the Level 1 scenarios will then be referred to as core damage in the procedures that follow.

The specification of the conditions assumed to represent core damage must be consistent with the VVER design features as well as with the capabilities of the analysis tools. For the Kalinin PRA, definition of core damage based on a maximum allowable fuel temperature is recommended. Other conditions that have been used are based on phenomena, such as UO_2 temperature limits, the triple point of the coolant, and the Zr-water autocatalytic temperature. For light water reactors, core damage has been defined when any one of the following conditions was met:

- Core maximum fuel temperature approaching 2200°F (1204°C)
- Core exit thermocouple reading exceeding 1200°F (649°C)
- Core peak nodal temperature exceeding 1800°F (982°C)
- Liquid level below the top of the active fuel.

Describing the conditions that characterize the core damage sequences is also necessary for the PRA. Experience has proven that if a Level 2 analysis is being contemplated, then it would be prudent to consider the interface between the Level 1 and Level 2 analyses while the Level 1 models are being developed. Typically, this interface is expressed in terms of plant damage states. Even if a Level 2 analysis is not performed, characterization of the damage states will provide significant insights into the nature of the Level 1 scenarios (e.g., which ones will involve successful containment isolation with containment heat removal available).

Each end state of the plant model event trees defines an accident sequence that results from an initiating event followed by the success or failure of various plant systems and/or operators responding to the accident. Each accident sequence has a unique "signature" due to the particular combination of system/operator successes and failures. Each accident sequence that results in core damage should be evaluated explicitly in terms of accident progression and the release of radioactive materials. However, since there can be many such sequences, it may be impractical to evaluate each one since this would entail performing thermal-hydraulic analyses and containment event tree split fraction quantification for each accident sequence. Therefore, for practical reasons, the Level 1 sequences are usually grouped into plant damage states or accident class bins. Each bin contains those sequences in which the following features are expected to be similar: the progression of core damage, the release of fission products from the fuel, the status of the containment and containment systems, and the potential for mitigating source terms. Plant damage state bins are used as the entry states (similar to initiating events for the plant model event trees) to the containment event trees, as described in Chapter 15.

7.1.3 Products

The products for this task are:

- a definition of the plant conditions that correspond to core damage and
- a definition of those plant conditions that represent successful termination of the accident scenarios.

7.2 Functional Analysis and System Success Criteria

The objectives of this task are to determine: (1) the functional capabilities of plant systems, (2) the functional relationships among plant systems, and (3) the success criteria for plant systems and components for use in the PRA. These activities are described below in general terms. More detailed guidance is provided in the references listed at the end of this chapter. [In particular, refer to Drouin (1987), NRC (1997), and NRC (1983).]

7.2.1 Relation to Other Tasks

As indicated in Figure 7.1, this task has extensive interactions with the following other PRA tasks.

Plant Familiarization. Prior to the initial site visit (see Chapter 2), the plant safety functions should be defined in Activity 1 below. This information is essential background material for the site visit.

During the site visit, a complete first draft of the Activity 2 dependency matrix (see below) must be completed.

Quality Assurance and Documentation. This task has obvious interfaces with QA requirements and provides input to the PRA documentation.

PRA Scope. Work beyond the full power operating state is not currently in the scope for the Kalinin PRA.

Core Damage Definition (refer to Section 7.1 above). If the risk results (see Section 11.1, Initial Quantification of Accident Sequences) are found to be heavily dependent upon the precise definition of the state of core damage, then additional Activity 3 calculations (see below) could help decide the optimal definition. This additional work may also suggest breaking that state into multiple states with varying impact. These calculations must take proper account of reactor decay heat to obtain valid results, especially with respect to timing. Such calculations are not in the current scope of the Kalinin PRA.

Initiating Event Analysis. Understanding of the Kalinin plant systems safety functions and interrelationships in Activities 1 and 2 may suggest redefinition of the initiating event groups.

Event Sequence Modeling (refer to Section 7.3 below). Activity 1 (below) defines the safety functions to be modeled in the event trees. Activity 2 helps to define the interrelationships among systems. Activity 3 is initially performed in concert with the preliminary development of the event sequence models. Judgments about the likely impact of Activity 3 assumptions on sequence-model structure and results guide the work. Later in the PRA, the task on Event Sequence Modeling (Section 7.3) will require additional Activity 3 work as needed to strengthen and simplify the models.

Systems Analysis. Activity 1 (below) defines the systems to be analyzed. Activity 2 provides the interrelationships among systems that define the fault tree structure, while Activity 3 provides the success criteria for systems models.

Human Reliability Analysis. Human reliability analysis is heavily dependent on Activity 3 (below), which defines the time available for various human actions and the extent of action required to cope with specific event sequences. Event Sequence Modeling, Human Reliability Analysis, and Activity 3 are deeply interrelated.

Initial Quantification of Accident Sequences. In this task, the results of all the modeling efforts, assumptions, and calculations are realized. Invariably, the results are considered as preliminary, requiring further analyses and refinements in the models/assumptions employed. Uncertainty analysis in the quantification task will require Activity 3 (below) calculations to assess the range of possible results. After the results are available, the highest frequency scenarios are analyzed by experienced analysts who look for expected contributors that have not reached the final results. Problems in modeling and success criteria will be found along with errors in computer input, calculations, etc. Extensions to the success criteria calculations of Activity 3 will be required to correct these problems.

7.2.2 Task Activities

Selection of success criteria is a continually evolving element in the PRA process (Bley, Buttemer, and Stetkar, 1988). Development of the success criteria involves investigations into the detailed timing of event sequences. These investigations utilize engineering analyses to calculate the time progression of plant parameters and human reliability analyses to help quantify operator response. Realistic engineering models can examine many possible scenarios of sequence starting conditions and equipment operability. As a result of developing such detailed information, it becomes possible to define more realistic equipment success criteria and to reduce the uncertainty in the time available to avoid damage. The objectives of this task must be conditioned by the conflicting goals of realism and costs. Although the success criteria of systems/components should be as realistic as possible, the effort needed to develop these criteria should be consistent with the risk importance of the particular system function.

A PRA is a large-scale scientific and engineering analysis performed for many purposes. The level of effort dedicated to any particular task must be balanced by its value. Perhaps no task in the PRA requires more balancing of costs and benefits than the skillful selection of realistic

success criteria. Success criteria should specify the minimum equipment needed for successfully mitigating the progression of a postulated accident. Success criteria also help to determine the effects of degraded system performance as well as to define the time available for recovery for each alternative success path potentially available to the operators. Defining realistic success criteria requires supporting analyses. The cost of neutronic and thermal-hydraulic analyses to support maximum realism in a PRA can be prohibitive. The cost of bounding analyses for traditional design basis analysis is substantial as well. If all possible variations in conditions that are modeled in the PRA were calculated, not in a bounding way but realistically, an enormous number of calculations would be required.

One must, therefore, begin with a preliminary judgment of importance, then use as realistic as possible evaluations for the issues of high importance. For items of lesser importance, conservative success criteria must be selected for each possible modeled condition. Note that realistic means more than "best estimate." Best-estimate calculations evaluate the most likely conditions. Realistic calculations must be a set of results for each set of conditions, weighted by the probability of that set representing the actual conditions. Frequently, the most risk-significant results are obtained from unlikely, but troublesome conditions.

Defining the success criteria must be an iterative process, starting with best judgments based on experience, knowledge of existing plant calculations, and knowledge of the plant PRA model and its effects on calculational difficulties. It progresses stepwise as systems analyses are completed, event trees are constructed and evaluated, and preliminary results are developed. How this task has been performed is not well documented in existing literature, perhaps because judgment plays a central role.

Selection of the final success criteria, which progresses by trial and confirmatory analysis, must be driven by the goals of the PRA. The criteria should be set to ensure that (1) the likelihood that the risk is higher than calculated as a result of errors in the success criteria is relatively small and (2) the leading risk contributors have a high probability of reflecting the true contributors, rather than being artifacts of arbitrarily pessimistic success criteria. In that way, the goals of the PRA can be achieved. The PRA becomes the foundation for the construction of a coherent safety basis for the plant. Such a basis permits rational evaluation of a wide range of issues by both regulators and plant staff. This task is broken down into three separate activities:

1. Determination of safety functions,
2. Assessment of function/system relationships, and
3. Assessment of success criteria.

The first two activities are straightforward, with clearly defined products (IAEA, 1992). The third involves substantial iterative work with other tasks to optimize the value of the PRA, while controlling costs. Work in this activity is often defined by requests from other PRA tasks.

7.2.2.1 Activity 1 — Determination of Safety Functions

Safety functions are any physical functions that can influence the progression of a postulated accident sequence by preventing or mitigating core damage or the release of radionuclides following core damage. The Reactor Safety Study (Rasmussen et al., 1975) introduced high-level safety functions: reactor subcriticality, core heat removal, reactor coolant system integrity, containment cooling, and fission product removal. In order to model safety functions in the event tree/fault tree PRA model, it is necessary to relate them to plant systems. The appropriate plant systems become the "top" events in the event trees. Note that some systems can provide multiple safety functions and that some functions can be supplied by multiple systems.

An example from a recent pressurized water reactor (PWR) PRA in the U.S. will illustrate the process. In Table 7-1, the high-level safety functions of the Reactor Safety Study are related to more detailed functions and finally to specific plant systems. In addition to the frontline systems listed in the table, a variety of support systems are required. The link to these systems is provided by the support to frontline system dependency matrix described in Activity 2. Finally, the specific plant systems modeled in the PRA will depend on the specific initiating event, the mode of operation prior to the initiating event, the time in that mode,

and the reliability of each system to provide the function.

For each of the initiating events identified in the task Initiating Event Analysis (Chapter 6), the safety functions that will be challenged or can be used to mitigate the initiating event should be identified during this activity. These will be the safety functions that will be modeled in the event tree analysis. The applicable piping and instrumentation diagrams, systems' descriptions, procedures (i.e., emergency, abnormal, and operating procedures or instructions), and design analyses should be identified and reviewed to ensure that the safety functions are correctly identified. The list of specific operating modes of Kalinin Nuclear Power Station systems that can provide these safety functions will be the product of this task.

7.2.2.2 Activity 2 — Assessment of Function/System Relationship

The frontline systems identified in Activity 1 provide the basis for this activity. All the support systems that are required for successful operation of each frontline system and its components are identified. A frontline system dependency matrix is prepared (as introduced in the task on Plant Familiarization, Chapter 2) which shows (train by train) the impact of support system failures on system operation. Next, a support system dependency matrix is prepared that shows (train by train) the impact of other support system failures on each support system train. Although this activity is performed during the plant visit described in Chapter 2, it is functionally part of this task. The detail and structure of the dependency matrices depend on the specific train-by-train design of the plant under investigation. The precise structure required for the Kalinin Nuclear Power Station will not be known until the detailed Plant Familiarization is carried out.

The dependency matrices form the underlying basis for the plant model. They describe the physical interrelationships among systems that are crucial to proper modeling and are often among the key factors in risk results. This is a relatively straightforward activity and adequate guidance is provided in NRC (1997) and Drouin (1987). To an experienced analyst, the dependency matrices provide the first indication of the plant risk. Interpretation of these relationships is an important part of Activity 3, where it provides the basis for many judgments that establish the success criteria.

7.2.2.3 Activity 3 — Assessment of Success Criteria

The success criteria are among the most important information needed in developing the scenarios in the event trees. The success criteria for the frontline systems and the timing of accident scenarios are determined in this activity. The success criteria specify the minimum equipment needed, determine the effects of degraded systems performance, and define the time available for recovery for each alternative success path available to the operators.

In general, the success criterion for a system changes with the initiating events and the preceding events in the event trees. Therefore, this task must be done in parallel with the event tree development task (see Section 7.3), and a systematic assessment will ensure that the success criteria have adequate bases. The assessment should account for the definition of core damage (see Section 7.1), decay heat, and the mission time. If the plant systems can prevent core damage from occurring during the mission time, then the accident sequence is considered successfully terminated. In many cases, calculations required for this Activity 3 actually establish the mission time.

The determination of success criteria must be based on tests, thermal-hydraulic analyses, other mechanistic analyses, and documented expert knowledge (Bley, Kaplan, and Johnson, 1992). In the U.S., the design-basis accident analyses form a useful source of existing calculations. "Credible" accidents are defined as single events (e.g., double-ended pipe ruptures, pump trip, pump seizure, etc.) followed by the most severe single active failure. The most severe of these (i.e., the one with the minimum margin to core damage) is the design-basis accident. In these calculations, the most pessimistic assumptions on plant parameters are made to bound the consequences of these accidents. Other analyses of the same or similar plants identified and collected in the task Plant Familiarization are also considered. Emergency procedures and other relevant procedures also provide information relevant to

the success criteria. Because of their ready availability, these calculations can be used as first approximations for establishing success criteria. At this stage, the criteria are generally conservative. The preexisting information will not be adequate to determine the success criteria and timing of all possible scenarios. Under the more severe conditions that occur in some PRA sequences (e.g., those with multiple failures), care must be taken to ensure that success criteria are still conservative. Otherwise, additional engineering analyses may be required.

The PRA team evaluates where such criteria may be so pessimistic that they will adversely affect the PRA results, and the team performs analysis to improve those success criteria. The team must also look for special conditions when the existing calculations are no longer conservative with respect to the considerations of the PRA model. In such cases, revised success criteria are mandatory.

The product of this task will include the success criteria for all frontline and support systems under all initiating event categories and the accident timing information that is an input to the human reliability analysis. This task also interfaces with the task Initiating Events. The backup documentation (see Chapter 3) should include the details of supporting thermal-hydraulic analysis done specifically for the PRA.

The first product of this task will be developed following the initial site visit and will be based upon the safety functions defined in Activity 1. Analysts will identify equipment for which success criteria will be required. They will identify existing analyses that could be used to set specific criteria and examine the potential problems in basing success criteria on these analyses. Bley, Buttemer, and Stetkar (1988) and Harrington and Ott (1983) provide a variety of examples to illustrate the kinds of analyses that are often performed to support PRAs. The examples suggest areas where new calculations could enhance the PRA. These results will form the basis for discussions during the second site visit which will bring the full expertise of the PRA team to bear on success criteria decisions.

Examples of calculational issues in support of success criteria definitions that have proved important in earlier PWR PRAs are provided below:

- Room heatup with no cooling;
- Time until steam generator dryout following loss of feedwater;
- Time until local accumulators would be exhausted following loss of instrument air for main steam isolation valves, steam generator relief valves, pressurizer power operated relief valves, etc.;
- Capability of various pumps to survive functionally with no cooling water, e.g., would the lube oil temperature stabilize at a safe temperature, would directing portable air blowers on the lube oil cooler help, perhaps if covered with wet rags;
- Possibility of pressurizer relief valves lifting following a variety of transients, accounting for realistic modeling of pressurizer steam space compression;
- Time until the feedwater storage tank is empty following a reactor trip under a variety of specific conditions, e.g., feedwater fails immediately and condenser steam sumps fail closed followed by uncontrolled automatic auxiliary feedwater flow; a similar case but operators control auxiliary feedwater flow, maintaining hot standby conditions; similar case but operators follow normal cooldown rate to cold conditions (i.e., when do they reach the switchover temperature for residual heat removal cooling); etc.;
- Bleed and feed behavior under a wide variety of equipment conditions and operator actions, focusing on minimum equipment required and cases in which bleed and feed cooling may not work if not initiated in time;
- Minimum success criteria for injection pumps following a variety of LOCAs; and
- Pressurized thermal shock calculations under a variety of conditions.

Table 7-1 Safety functions identified in a recent PWR PRA

High-Level Safety Function	Lower-Level Safety Function	Plant Systems
Reactor subcriticality		•Rod control system •Passive-moderator density for large loss-of-coolant accidents (LOCAs)
Core heat removal	Primary system flow and mixing	•Reactor coolant pumps
	Primary system bleed and feed	•Charging system •Pressure relief system
	Secondary heat removal	•Main steam system (steam dumps, atmospheric steam dumps) •Auxiliary feed system •Main condensate system •Main feed system •Service water system
	Long-term shutdown cooling	•Residual heat removal system •Main condensate •Main condenser
Reactor coolant system integrity	Leak prevention/isolation	•Reactor coolant loop •Pressure relief system, including block valves •Reactor coolant pump seals
	Primary system depressurization	•Pressure relief system •Main steam system (steam dumps, atmospheric steam dumps) •Auxiliary feed system •Main condensate system •Main feed system •Service water system
	Primary system makeup	•Charging system •High-pressure injection system •Low-pressure injection system
Containment cooling		•Containment spray •Containment fan coolers •Passive--containment heat sinks
Containment fission product removal		•Containment spray •Passive--steam generators if melt due to steam generator tube rupture

This list is only a sampling of analyses that have been performed to support PRAs. In the following section, examples of "hand" calculations, simple computer solutions, and the use of elaborate thermal-hydraulic codes are discussed. The required analyses vary on a plant-by-plant basis depending on the availability of existing calculations, specific vulnerabilities at each plant, the availability of alternative ways to satisfy safety functions, and the tolerable level of conservatism in the final results. The major responsibility of the analysts in this task is to respond to the requests for information generated in the other project tasks, subject to the concurrence of the project manager. The amount of supporting analysis is always a trade-off between technical rigor and the associated value to the users of the PRA.

7.2.2.4 Additional Guidance

Early work in PRAs, most notably the Reactor Safety Study (Rasmussen et al., 1975), focused on large issues--bringing the probabilistic viewpoint to the field of safety assessment, moving from worst-case bounding analyses toward realism, building the first large-scale models of integrated plant performance, developing the methods to structure such models (e.g., event trees and fault trees), and analyzing events well beyond the design basis of nuclear power plants (e.g., degraded core phenomena and the progression and impact of offsite effects of radionuclide releases). Later, as the field matured, areas of conservatism, subtle areas of optimism, and areas where more thorough analysis could enhance understanding have been revealed and studied.

In the development of PRA event sequence models, success criteria are established for systems and components and for specified operator actions (i.e., top events explicitly shown in the event trees) that can prevent core damage or containment failure. In their simplest and earliest form, success criteria tell us the minimum equipment configuration (e.g., *n* of *m* pumps must operate) required to ensure success of a given safety function for all credible conditions. However, the question remains whether failure to meet conservative success criteria ensures core melt or whether meeting those criteria ensures success for all possible conditions. Because PRA seeks to quantify risk (i.e., to quantify what credible means), more general success criteria are needed. These new success criteria must identify the length of time the plant can survive in various equipment configurations--that is, they must identify the time available for specific operator actions or equipment recovery. It is not possible to know the available time exactly because of variability in plant conditions and because the team's knowledge is imperfect. This uncertainty is properly expressed as a probability distribution.

To establish success criteria, analysts must have well-founded technical knowledge of how specific plant equipment and operators respond to a very broad range of operational and accident scenarios. One can develop an understanding only through a combination of operational experience, tests, and analysis. Events that are expected to occur quite frequently would normally fall into the operational experience category. Events that are included in the traditional licensing design basis are often covered by testing (sometimes generic in nature) and conservative analyses. These analyses used methods that are approved by regulatory authorities and typically include mandated assumptions, e.g., the existence of a single active failure. In the development of PRA models, many scenarios lie outside the rather narrow traditional licensing basis of the plant. Therefore, they are not included in the accident analyses contained in the plant-specific safety analysis report. Such scenarios might involve the occurrence of multiple failures, the availability of both nonsafety- and safety-related equipment, and severe accident scenarios. These are accidents which extend well beyond the design basis and address the performance of equipment that can potentially mitigate the accident consequences following core damage.

Ideally, the results of a wide range of analyses (primarily thermal-hydraulic and structural and occasionally electrical engineering) would be available that use best-estimate data and correlations and can cover the very large number of scenarios considered in a PRA. Unfortunately, this is seldom the case, and additional analyses are often needed to support the PRA model. The additional analyses can range from simplified mass and energy balances done by hand calculations or small microcomputer-based programs to very sophisticated computer-based models that may include momentum effects,

complex control system interactions, and a considerable amount of empirical data.

In recent years, analysts in the nuclear industry have focused on elaborate computer codes that have permitted solution of many complex phenomena. Along the way, the value of more straightforward calculations has often been forgotten. Many questions concerning event sequence timing are simple thermal-hydraulic problems. All too often, PRA analysts have shied away from refining success criteria because of the cost of running sophisticated codes when low-cost, simple calculations would have adequately answered the question at hand. For example, questions relating to when the PWR steam generators will boil dry with no feedwater, how long will it take to refill the pressurizer following a severe overcooling event, how does boiling water reactor containment pressure and temperature vary following vessel isolation, or how quickly do rooms heat up with reduced cooling capability, and when does that cause equipment failures.

The basic data needed for many of these calculations include the American Society of Mechanical Engineers steam tables (Keenan and Keyes, 1950), the critical mass flux of saturated steam and water developed by F. J. Moody (1965), the decay heat rates outlined in the American Nuclear Society Guide 5.1 (ANS, 1994), and plant-specific data (power, volumes, pump curves, etc.). More complex computer calculations using state-of-the-art thermal-hydraulic and neutronic codes are also required at times, but the simpler analysis should be considered first.

The recommended approach to follow in selecting engineering analyses to support PRA recognizes real-world budget and schedule constraints, while maintaining adequate depth on the most significant scenarios. It proceeds as follows:

- Use conservative safety analyses on most scenarios;
- Apply simplified analyses to develop preliminary, less conservative success criteria for scenarios that appear particularly sensitive;
- Document the analyses and assumptions;
- Evaluate the point estimate frequencies of the entire PRA model;
- Review results to identify the dominant risk contributors; and
- Revise the analysis, as required, to obtain realistic and accurate results.

The preliminary risk results are reviewed to identify the dominant risk contributors. Areas where it is important and justifiable to evaluate uncertainties or to perform more sophisticated analyses to better define success criteria are then identified. The goal is to understand safety quantitatively, not just to bound the results. Although the engineering analyses are "best estimate" and deterministic in nature, there are physical and analytical uncertainties no matter how sophisticated the analysis. Sensitivity studies permit evaluation of those uncertainties as well as the variability associated with plant operation.

7.2.3 Products

The Activity 1 letter report will define the safety functions to be modeled as top events in the event sequence analysis and the systems that provide those functions. This report is required as preparation for the site visit for the task on Plant Familiarization (Chapter 2).

The Appendix to the PRA Report (see Chapter 3) will describe the plant dependency matrix that is produced in Activity 2. This report should be completed before the conclusion of the first site visit.

The Activity 3 initial letter report will identify equipment for which success criteria will be required, existing analyses that could be used to set specific criteria, and new analyses that may be required.

The Activity 3 letter report will define new supporting analyses for initial success criteria selection. This report should be completed before the conclusion of the second site visit.

The Activity 3 letter report will define success criteria resulting from the initial modeling effort.

The Activity 3 letter reports will provide the results of calculations requested by other tasks. These reports will be part of the project backup

documentation (see Chapter 3), and some will be used in preparation of the PRA Report.

7.3 Event Sequence Modeling

The objectives of this task are: (1) to determine the range of possible plant and operator responses to a wide variety of upset conditions and (2) to develop event trees for all initiating event categories that are defined in the task Initiating Event Analysis (Chapter 6). The event trees must track sufficient information to permit assignment of each event tree sequence to one of the defined plant damage states. These activities are described below in general terms. More detailed guidance provided in the references listed at the end of this chapter.

The event sequence model is the heart of the PRA. It is the high-level model of how the plant works on a functional basis. It relates functions to plant systems and provides some information on the time sequence of functional interactions. At lower levels, these functions are related to specific plant components and the interrelationships among those components. While some PRAs develop event trees directly, this procedure guide requires the intermediate stop of constructing event sequence diagrams (ESDs). These ESDs are more transparently linked to plant operations and responses described in the operating instructions (especially the emergency operating procedures). They are suitable for review by plant operators and engineers as well as PRA specialists. They provide documentation for the more abstract event tree models and provide a lasting record of the simplifications required to develop event trees suitable for quantification. Familiarity with the ESDs can ensure that individual systems, data, and human reliability analysts are aware of the role of their work within the overall structure of the PRA model.

7.3.1 Relation to Other Tasks

As indicated in Figure 7.1 this task has extensive interactions with the following:

Plant Familiarization. During the initial familiarization task, the preliminary ESDs based on the relevant emergency procedures for transients, loss-of-offsite power, and LOCAs should be developed. The mitigating functions and the systems associated with the functions should be tabulated.

PRA Scope. Work beyond the full power operating state is not currently in the scope for the Kalinin PRA. For studies that consider additional states, new ESDs and event trees will be required.

Initiating Event Analysis. Event trees must be developed or applied to each initiating event group. Analysis of the impact of event tree questions on each group may lead to a redefinition of the groups, combining groups when plant response is sufficiently similar and breaking apart groups or reassigning specific initiating events as new insights warrant them. Details of each specific initiating event that can affect systems modeled in the event tree must be properly accounted for.

Functional Analysis and Systems Success Criteria (refer to Section 7.2 above). This task and the current task are highly coupled and performed in an iterative fashion. In the task Functional Analysis and Systems Success Criteria, Activity 1 (Determination of Safety Functions), defines the safety functions to be modeled in the event trees. Activity 2 (Assessment of Function/System Relationships) provides the defining interrelationships among systems. Activity 3 (Assessment of Success Criteria) is initially performed in concert with the preliminary development of the event sequence models. Judgements about the likely impact of these assumptions on results and model structure guide by the early work. Later in the project, the current task will prompt additional Activity 3 work as needed to strength and simplify the models.

Systems Analysis. The event tree sets the boundary conditions for the system models. As part of this activity, a qualitative dependency analysis is performed which searches for dependencies to insure that all significant dependencies are reflected in the final models. Model enhancements to more accurately reflect functional, spatial, and human-induced interactions may be required as a result.

Human Reliability Analysis. Human reliability analysis (HRA) is heavily dependent on event sequence modeling. Proper consideration of factors affecting the plant and human context for HRA, including dependencies among human actions, will affect the structure of the event trees.

Conservative, unrealistic systems models cannot be supported with meaningful HRA. Modeling human actions under situations that will not occur is an exercise in irrelevance.

Initial Quantification of Accident Sequences. In this task, the results of all the modeling efforts, assumptions, and calculations are realized, and invariably, the results at this point are not satisfactory. After the results are available, the highest frequency scenarios are analyzed, and experienced analysts look for expected contributors that have not reached the final results. Problems in modeling and defining success criteria will be found along with errors in computer input, calculations, etc. Revisions to the event tree structures and definitions of top events will almost certainly be required. Project management must anticipate substantial effort for review and revision.

Fire, Flood, and Seismic Analyses. Event trees from the internal events analysis will generally serve to model fire-, flood-, and seismic-induced sequences (not shown in Figure 7.1). Because these types of initiating events can induce multiple internal initiating events and affect multiple systems helpful for recovery, revisions to the event tree structures and definitions of top events may be required.

7.3.2 Task Activities

The process of building the event sequence models is inexact and is not likely to be completely codified. The analyst must balance many competing factors: completeness, ease of modeling, efficiency of use for specific risk management applications, rigor, flexibility, etc. A little extra effort in the beginning to understand the range of possible applications--those anticipated as well as those that could eventually be needed--can save enormous effort and cost later.

The delineation of Level 1 accident sequences ends with the determination of the status of the core as safe or damaged as described for the task Core Damage Definition. For core damage cases, each sequence is further assigned to a plant damage state. These plant damage states are defined so that all sequences within a state are essentially identical with respect to the questions addressed in the Level 2 model. The assumption in the Level 2 analysis will be that these sequences are identical.

Plant components modeled in a PRA are generally assumed to be fully operational or nonoperational. Differentiation is not usually made between full and partial operation of a component. Therefore, PRA methodology does not usually take into account degraded (e.g., valve partially open) or enhanced performance of a system component (e.g., pump operating near runout conditions). Precise definition of component functional failure and the possibility of modeling degraded states requires careful consideration of the potential impact of these degraded states.

The International Atomic Energy Agency (IAEA) PRA procedures guide (IAEA, 1992) provides a more prescriptive alternative to accident sequence event tree development. The more flexible ESD approach is recommended for the Kalinin PRA to account for any special design characteristics of the Kalinin VVER-1000 that might affect risk. Plant-specific consideration of success criteria may indicate the need to model degraded functionality. Additionally, the ESD approach has the potential to more thoroughly document the basis for the event sequence model than for the functional event tree/systemic event tree approach recommended by the IAEA.

This task is broken down into three separate activities:

1. Develop fundamental ESDs,
2. Abstract selected PRA event trees from the fundamental ESDs,
3. Test remaining initiating events against fundamental ESDs and existing event trees.

These three activities are described in more detail below. They form a stepwise approach to developing the event trees with minimum duplication of effort. The approach is accessible for review by a wide range of experts. Moreover, it can clearly explain the simplifications necessary to develop practical, useful, quantifiable models. This event sequence modeling task forms the underpinning of the entire PRA model and is, therefore, closely linked with other tasks in the PRA.

7.3.2.1 Activity 1 — Develop Fundamental Event Sequence Diagrams

An event sequence model is used to identify the many possible plant response sequences to each initiating event. Depending on various combinations of plant equipment and operator response success or failure states, the event sequences will either be terminated with no core damage or will lead to core damage and various degrees of plant damage, defined as plant damage states. The ESDs are generally developed in cooperation with operators at the plant to ensure the model represents the plant "as built" and as operated.

The first step in plant modeling for a PRA is to develop a "general transient" ESD, i.e., a model for all events in which high pressure can be maintained in the primary system, active core cooling is required, and high pressure makeup may be needed. This is the most general PRA model, one that can be specialized to address most transients and accidents. This ESD should be directly applicable to many initiating events, e.g., small LOCA, loss-of-offsite power, reactor trip, and turbine trip.

The second fundamental ESD is that of a large LOCA. For most PWRs, the large LOCA is the most strikingly different ESD because low pressure injection is required, control rods are not required for nuclear shutdown, and only long-term cooling is required. Thus, at least this one new ESD will be required.

7.3.2.2 Activity 2 — Abstract Selected PRA Event Trees from the Fundamental ESDs

The general transient ESD should provide a complete model for a number of initiating event groups including reactor trip, loss of main feedwater, turbine trip, loss-of-offsite power, and loss of primary flow. The ESD displays the basic relationships between the systems and their impact on the overall plant status and relates those actions required to mitigate the effects of the plant disturbance caused by the initiating event to the steps in the plant emergency procedures. The event trees are developed from the ESDs. The specific actions key in determining the accident progression are identified in the ESDs and grouped into top events in the corresponding event tree. This grouping of actions is displayed in the ESDs to document the event tree development. Since the ESD does not directly lend itself to accident sequence quantification, construction of the event trees is a necessary step. A description of the included actions and the success criteria for each top event must be developed in detail with the event tree structure. The success criteria identifies the analysis boundary conditions required for the systems analysis tasks. Finally, each sequence in the event tree must be assigned to its plant damage state.

The frontline system response to several different initiating event categories may be similar. Therefore, the same event sequence models may be used to quantify the risks from more than one such initiating event category, although some differences in the fault trees and data may be required for proper quantification. These differences reflect the different conditions imposed by the specific initiating event category.

7.3.2.3 Activity 3 — Test Remaining Initiating Events against Fundamental ESDs and Existing Event Trees

The PRA team working on ESD development will review each remaining initiating event against the general transient and large LOCA ESDs, identifying any structural changes that may be required and defining any special conditions that must be accounted for when the individual event trees are constructed. The exact number of ESDs and event trees required for the PRA will be determined at this time.

7.3.2.4 Additional Guidance

Development of the event sequence model is an exercise in addressing a wide variety of open-ended questions. An insightful and experienced analyst must lead the work integrating knowledge of potential accidents, thermal-hydraulic and neutronic response, plant systems and operations, and systems analysis for PRA. Despite efforts to formalize the process, much will remain subjective due to the open-ended nature of the problems to be solved. Documentation of assumptions, simplifications, and approximations, and the reasons for them is essential for the understanding and future use and modification of the study.

Models developed with an eye toward flexibility will serve their owners well in the long term. For example, if Level 1 models (NRC, 1983) anticipate Level 2 needs, the Level 2 PRA will require far fewer costly revisions to the Level 1 model and far less tortured arguments to tie the complete analysis together. System fault trees built originally for risk evaluation and identification of dominant contributors will need to be expanded, separating failure rate into demand- and time-based elements, if test schedule optimization is desired. Definitions of systems' boundaries and decisions concerning the extent of fault tree versus event tree models will affect the ease of testing the effects of design changes on risk. Generally, changes to the database are easier to implement than changes to the fault trees, and changes to a fault tree are easier than changes to an event tree. Many such trade-off decisions must be made during the PRA development.

To get a better understanding for the thought process involved in the event sequence modeling task, consider a transient initiating event. The general transient ESD is used to model events that require a reactor trip, turbine trip, and decay heat removal for successful mitigation. The normal plant responses for these initiating events are:

1. Plant conditions result in a demand for a reactor trip, turbine trip, and generator trip. Sequences with a successful trip are modeled in the event sequence model. Unsuccessful reactor trip sequences are modeled in a separate transients-with-failure-to-scram model.

2. The exact sequencing of reactor, generator, and turbine trips are design specific and lead to different requirements for steam relief.

    a. If a turbine trip and reactor trip occur first and are nearly simultaneous, steam generator pressure rises due to the loss of load (turbine trip) and the addition of core decay heat as well as stored heat. Typically, condenser steam dump valves open automatically to control the primary system at the no-load T_{avg} temperature by passing steam to the plant condensers. If the condensers are not available, secondary steam relief is achieved with the steam generator atmospheric steam dumps.

    b. If a generator trip occurs first, the same sequence occurs.

    c. If a reactor trip occurs first and a turbine and generator trip are delayed, the turbine removes the initial decay heat, reducing the need for steam bypass.

3. Feedwater is added to the steam generators by the auxiliary or emergency feedwater pumps (main feedwater valves may isolate depending on plant-specific design features) to make up the steam generator inventory lost by dumping steam.

4. As reactor decay heat decreases and plant conditions return to normal, primary system temperature is maintained at the no-load T_{avg} value by the action of the condenser steam dump valves or the atmospheric steam dumps, or through system steam loads. The steam generator water level is maintained by the water level control system or by operator action, and recovery from the plant trip commences.

Failure of a turbine trip results in an excessive steam demand and could result in overcooling the primary system. Automatic steam line isolation should then occur because of protection system actuation. Failure of steam line isolation and turbine trip leads to a rapid overcooling of the primary, automatic initiation of the emergency core cooling system equipment due to the resulting decrease in primary system pressure, and a possible challenge to the reactor pressure vessel integrity because of pressurized thermal shock should the RCS be repressurized when the vessel wall is overcooled.

Failure of auxiliary feedwater requires operator action to restore main feedwater or establish low pressure condensate flow to the steam generators. Failure of the steam generator feed systems requires operator action to initiate the

"feed and bleed" mode of cooling the primary and the reactor core. Failure of this mode of cooling results in a high pressure core melt because of loss of all heat removal options.

If cooling water systems fail, cooling is lost to key equipment and, in some cases, this can induce subsequent LOCAs through damage to primary system equipment.

Having reached this point successfully, long-term cooling needs must be addressed. Finally, core melt is assumed to occur for those event sequences in which all core cooling is lost or a LOCA occurs with no safety injection. The operation of the containment building cooling and fission product removal systems are analyzed in the core melt sequences since it is necessary to remove decay heat and to minimize the fission product release for these core melt sequences.

7.3.3 Products

1. A set of ESDs that document the range of possible plant and operator response to a range of upset conditions.

2. A complete set of event trees to quantify all initiating events. This product must include complete definitions of top events to support system analysis and HRA. Each event tree must be developed from the relevant ESD showing which ESD elements are combined into single event tree top events, justifying the event tree model as an abstraction of the ESD based on characteristics of the initiating event and approximations well supported by probabilistic and engineering argument.

7.4 References

ANS, "American National Standard for Decay Heat Powers in Light Water Reactors," American Nuclear Society Standards Working Group, ANSI/ANS-5.1-1994, American Nuclear Society, 1994.

Bley, D. C., S. Kaplan, and D. H. Johnson, "The Strengths and Limitations of PSA: Where We Stand," *Reliability Engineering and Systems Safety*, *38*, pg. 3-26, 1992.

Bley, D. C., D. R. Buttemer, and J. W. Stetkar, "Light Water Reactor Sequence Timing: Its Significance to Probabilistic Safety Assessment Modeling," *Accident Sequence Modeling: Human Actions System Response, Intelligent Decision Support*, G. E. Apostolakis, P. Kafka, and G. Mancini, editors, Elsevier Applied Science, 1988.

Drouin, M., et al., "Analysis of Core Damage Frequency from Internal Events: Methodology Guidelines," Volume 1, NUREG/CR-4550, September 1987.

Harrington, R. M., and L. J. Ott, "The Effect of Small Capacity, High Pressure Injection Systems on TQUV Sequences at Browns Ferry Unit One," NUREG/CR-3179, Oak Ridge National Laboratory, September 1983.

IAEA, "Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1)," Safety Series No. 50-P-4, International Atomic Energy Agency, 1992.

Keenan, J. H., and F. G. Keyes, *Thermodynamic Properties of Steam,* John Wiley, New York, November 1950.

Moody, F. J., *Maximum Flow Rate of a Single Component, Two-Phase Mixture,* American Society of Mechanical Engineers, New York, February 1965.

NRC, "The Use of PRA in Risk-Informed Applications," NUREG-1602, Draft Report for Comment, June 1997.

NRC, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, U.S. Nuclear Regulatory Commission, January 1983.

Rasmussen, N. C., et al., "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, October 1975.

8. SYSTEMS ANALYSIS

The second analytical element in a Level 1 probabilistic risk assessment (PRA) is the systems analysis (refer to Figure 1.3). Systems analysis consists of three interrelated tasks--namely, system modeling, subtle interactions, and spatial interactions. This is shown on the flow chart in Figure 8.1. The first of these tasks is the heart of the systems analysis. The objective of the task on system modeling is to develop the system logic models (e.g., through the use of fault trees) that will be used to support the event sequence quantification. The objective of the task on subtle interactions is to identify and to explicitly model subtle interactions that could potentially cause single or multiple component the U.S., the design-basis accident analyses form a useful source of existing calculations. "Credible" accidents are defined as single events (e.g., double-ended pipe ruptures, pump trip, pump failures, which are neither covered by a common-cause failure analysis nor addressed in the dependency matrix. The objective of the task on spatial interactions is to identify potential environmental hazard scenarios at the plant.

Figure 8.1 shows the important relationships between the tasks under systems analysis and the other major components of the PRA. These relationships are explored in more detail in each of the sections describing the three tasks. System modeling is discussed in Section 8.1, subtle interactions in Section 8.2, and spatial interactions in Section 8.3.

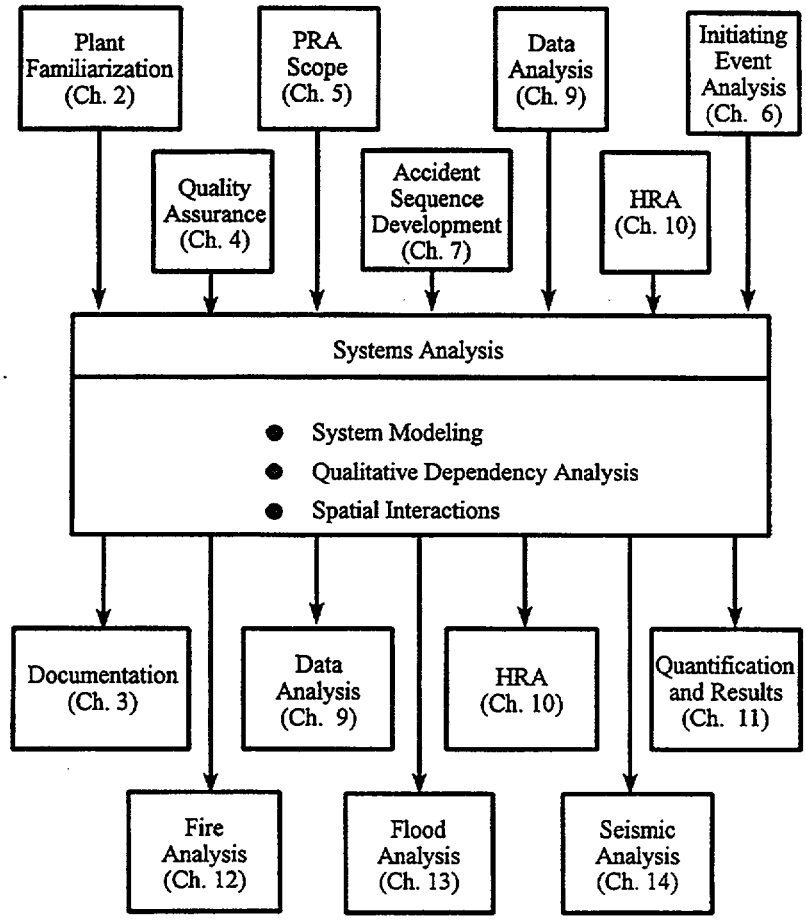


Figure 8.1 Relationships between systems analysis and other tasks

8.1 System Modeling

The goal of this task is to develop the system logic models necessary to support the event model activities, including possibly the determination of the frequency of selected initiating events, along with the supporting documentation.

This task consists of constructing models for those systems to be considered in the PRA. The most usual element of these models is the failure or success of a system. The details of the events can be analyzed through one of a number of system modeling techniques (i.e., fault trees, state space diagrams, reliability block diagrams, or go charts). These techniques are described below in general terms. More detailed guidance is provided in the references listed at the end of this chapter. [In particular, refer to Drouin (1987) and NRC (1997).] In addition, an excellent reference to systems analysis can be found in Section 5 of Ericson et al. (1990). Fault tree analysis is the method for developing system models in this study.

8.1.1 Relation to Other Tasks

As indicated in Figure 8.1, the System Modeling task has extensive interactions with all the other PRA tasks:

Plant Familiarization. This task obviously provides the key source material for the system models.

Quality Assurance and Documentation. The System Modeling task has obvious interfaces with QA requirements and provides input to the PRA documentation.

PRA Scope. The systems of concern are those needed to perform the functions modeled in the PRA. For the Kalinin PRA, this means the systems modeled for the full power operating state.

Initiating Event Analysis. The systems analysis can possibly identify additional initiating events related to a particular system.

Accident Sequence Development. The sequence development task defines the boundary conditions for the system models. The minimum success criteria for systems to perform their function are established here. System dependencies must be included in the system models.

Subtle Interactions and Spatial Interactions. The System Modeling task defines requirements for and receives feedback from these other two tasks of the Systems Analysis.

Data Analysis. The component availability used to quantify the system models comes from the data analysis. In some cases, the initiating event frequencies found in the data analysis can come from system models.

Human Reliability Analysis. Human error events are taken into account in the system models, and the models provide feedback to the HRA.

Quantification and Results. The Systems Analysis task must be completed before the quantification and results of the PRA are completed.

Fire, Flood, and Seismic Analyses. As indicated in Figure 8.1, the system models developed for the internal events PRA will also serve for the external event analysis, although additional models or considerations may be needed.

8.1.2 Task Activities

Before any fault trees are developed, it is necessary to have a very good understanding of the system operation, the operation of the system components, and the effects of component failure on system success. Sources of information that the analyst can use to gain this understanding of the normal and emergency operation of the systems are: system training notebooks, system operating instructions, system surveillance instructions, and maintenance procedures. It is also important for the analyst to understand the system requirements within the context of the event tree model and the event tree headings.

The analysis boundaries are based on functionality. Therefore, it is important to clearly define the boundaries of the system, which will likely be different than the boundaries specified by the normal system descriptions. For example, if

a portion of a service water line serves only the pumps of the residual heat removal (RHR) system (and failure of that line would only impact the RHR system), then the availability of that line would be analyzed as part of the RHR system. The boundaries of the RHR system for the purpose of this analysis would, therefore, include that specific service water line.

Not all systems are analyzed to the same level of detail. The appropriate level of analysis detail is governed by the importance of the system in relation to its role in preventing or delaying core damage and the complexity of the system. An important consideration is the depth at which the supporting data best provides a quantitative characterization of the unavailability of the system.

The analyst should examine all available information collected in Plant Familiarization in order to gain insights into the potential for independent or dependent failures in the systems and the potential for system interactions. The information contains descriptions of all types of failures that have occurred at the plant and possibly at similar plants.

The development of support system-to-support system and support system-to-frontline system dependency matrices, along with a comprehensive set of explanatory notes that clearly depict the functional relationship between systems and system trains, is needed early on in this analysis. These matrices may have been drafted as part of the task Plant Familiarization but should be updated and kept current as part of the present task. A simplified example of a dependency matrix is included as Figure 8.2. More details can be found in Chapter 2.

A schematic for each system needs to be developed. However, the plant drawings are usually very detailed, containing considerably more information than is required in the systems analysis task. A simplified system schematic that defines the system to a level of detail commensurate with the needs of the system analyst is, therefore, necessary.

To facilitate the analysis task, a table is created by the analyst that depicts the status of the system components (i.e., pumps and valves) under at least two sets of conditions:

1. when the plant is operating normally (i.e., the initial conditions for the analysis) and
2. when the system responds to a plant initiating event.

Note that multiple cases may be necessary in defining the desired component status to all of the plant events of interest.

The analyst should also determine the potential for each system to initiate an accident, should the system inadvertently (or prematurely) operate, malfunction, or fail. These will be compared with the identified initiators (see Chapter 6), and new plant initiators will be added, as appropriate. The possible identification of initiating events under this task is meant to complement the activity described in Chapter 6. In other PRA studies, the system analysts have often developed a level of understanding of the systems and have provided insights into the modes of system failure that make such a complementary activity beneficial.

Fault tree analysis is a common method used for representing the failure logic of plant systems. An undesired state of a system is specified, and the system is then analyzed in the context of its environment and operation to find all the credible ways in which the undesired state could occur. The fault tree is a graphic representation of the various combinations of events that would result in the occurrence of the predefined undesired event. The events are such things as component hardware failures, human errors, maintenance or test unavailabilities, or any other pertinent events that could lead to the undesired state. A fault tree thus depicts the logical interrelations of basic events that lead to the top event of the fault tree. These interrelations usually can be depicted as combinations of events in parallel or series, developed to the point where the data are best defined. This may be at the component level, subassembly level, or even, in very specific cases, at the system or subsystem level. The system analysts must, therefore, work closely with the data analysts to determine the level at which the basic event data are best defined. For example, successful operation of a system may require the operation of a sensor and an associated signal processing unit that together

		SUPPORT SYSTEMS										FRONTLINE SYSTEMS						
		DIESEL GENERATOR I	DIESEL GENERATOR II	4160V ACI	4160V ACII	HVAC I	HVAC II	SERVICE WATER I	SERVICE WATER II	COMPONENT COOLING WATER I	COMPONENT COOLING WATER II	EMERGENCY FEEDWATER PUMP A	EMERGENCY FEEDWATER PUMP B	CONTAINMENT SPRAY SYSTEM	SAFETY INJECTION SYSTEM	SWING PUMP	RECIRCULATION SYSTEM	RCP SEALS
SUPPORT SYSTEMS	OFFSITE POWER			1	1													
	DIESEL GENERATOR I			1														
	DIESEL GENERATOR II				1													
	4160V ACI			–		X		X		X		X		X	X		X	
	4160V ACII				–		X		X		X					X		
	HVAC I			2		–						2	2	2	2			
	HVAC II				2		–									2		
	SERVICE WATER I	X						–		X							3	
	SERVICE WATER II		X						–		X							
	COMPONENT COOLING WATER I					X				–				4	4		4	X
	COMPONENT COOLING WATER II						X				–					4	5	

NOTES:

1. WITH LOSS OF OFFSITE POWER, 4160VAC POWER IS SUPPLIED BY THE DIESEL GENERATORS
2. FAILURES OF THIS EQUIPMENT MAY OCCUR SEVERAL HOURS AFTER LOSS OF HVAC DUE TO ROOM HEATUP
3. THE RHR PUMP IS COOLED BY SERVICE WATER, DIVISION I
4. THE CONTAINMENT SPRAY PUMP, SAFETY INJECTION PUMP, SWING PUMP, AND THE RHR HEAT EXCHANGER REQUIRE COOLING DURING RECIRCULATION HEAT REMOVAL
5. CCW II IS THE ALTERNATE SOURCE OF COOLING FOR THE RHR HEAT EXCHANGER

Figure 8.2 Example of dependency matrix

constitute a complete logic channel. However, the data analysts may have developed the data only to the level of the logic channel, in which case only a single basic event (at the logic-channel level) is appropriate in the fault tree. Alternatively, the data may have been expressed in such a manner that makes more than one basic event appropriate. It has been shown that due to inherent conservatisms in most databases, developing data at too fine a level (e.g., resistors, capacitors, and other electronic components in an amplifier) may result in an inaccurate determination of the performance of the overall assemblage. For some systems (for example, balance of plant systems), the available data may be best defined at a rather high level, such as at the train or system level.

An example of a simple fault tree is included as Figure 8.3. The system represented in the fault tree is a backup cooling system represented by top event "BU" in an event tree. Both pumps in this simple example are initially in standby and each represents 100 percent capacity for delivering the required flow. Each train is tested periodically using a bypass line, which would render that train inoperable if left in the incorrect position following the test. The two trains share a common suction valve and a common discharge check valve. Motive power, control power, room cooling, actuation signals, and all other support are all assumed available. This assumption is made only to simplify the discussion; it would not be appropriate in the PRA system models.

Another example is taken from an actual PRA application (Chu et al., 1994) that utilized the Integrated Reliability and Risk Analysis System (IRRAS) computer code for fault tree quantification. This example (Figure 8.4) addresses a portion of the logic developed for a fluid system. This system, called the Inside Spray Recirculation System, requires both trains to be operable for the success of the particular top event considered. Transfers to other fault trees that are used to develop the logic further (e.g., "failure of 120V DC bus 1A") are indicated by triangles.

The general techniques for constructing, manipulating, and quantifying fault trees are described in Haasl et al. (1981). However, the following issues merit special consideration in the development of fault trees:

1. In order to facilitate consistency of the individual fault tree analyses, it is necessary that the definition of system boundaries and the conventions used to represent logic symbols, event coding, and representation of human errors and common cause failures be a priori specified for all the fault tree analysts. It is suggested that one system analysis be prepared before the fault trees for the other systems are started to serve as a guide. Human actions that occur following the initiating event are properly treated at the event tree level. The only human actions that should be included as events in the fault trees are those actions that potentially follow test and maintenance.

2. All assumptions made while constructing a fault tree should be documented, together with the source (and revision number) of all design information used. In this way, consistency will be promoted throughout the analysis and traceability will be maintained.

3. When systems are not modeled in detail and reliability data at the system level are used, failure events that are common with other systems should be separated out and explicitly considered.

4. Computerized methods should be used for handling the solution and quantification of fault trees to ensure consistency, comprehensiveness, efficiency, and quality.

5. It is strongly recommended that clear and precise definitions of system boundaries be established before the analysis begins. Any modifications to these definitions should be made known to all the other system analysts during the course of the analysis. The analysis boundary definitions should be included in the final documentation covering the systems modeling. The interface points between frontline systems and various support systems could, for example, be located as follows:

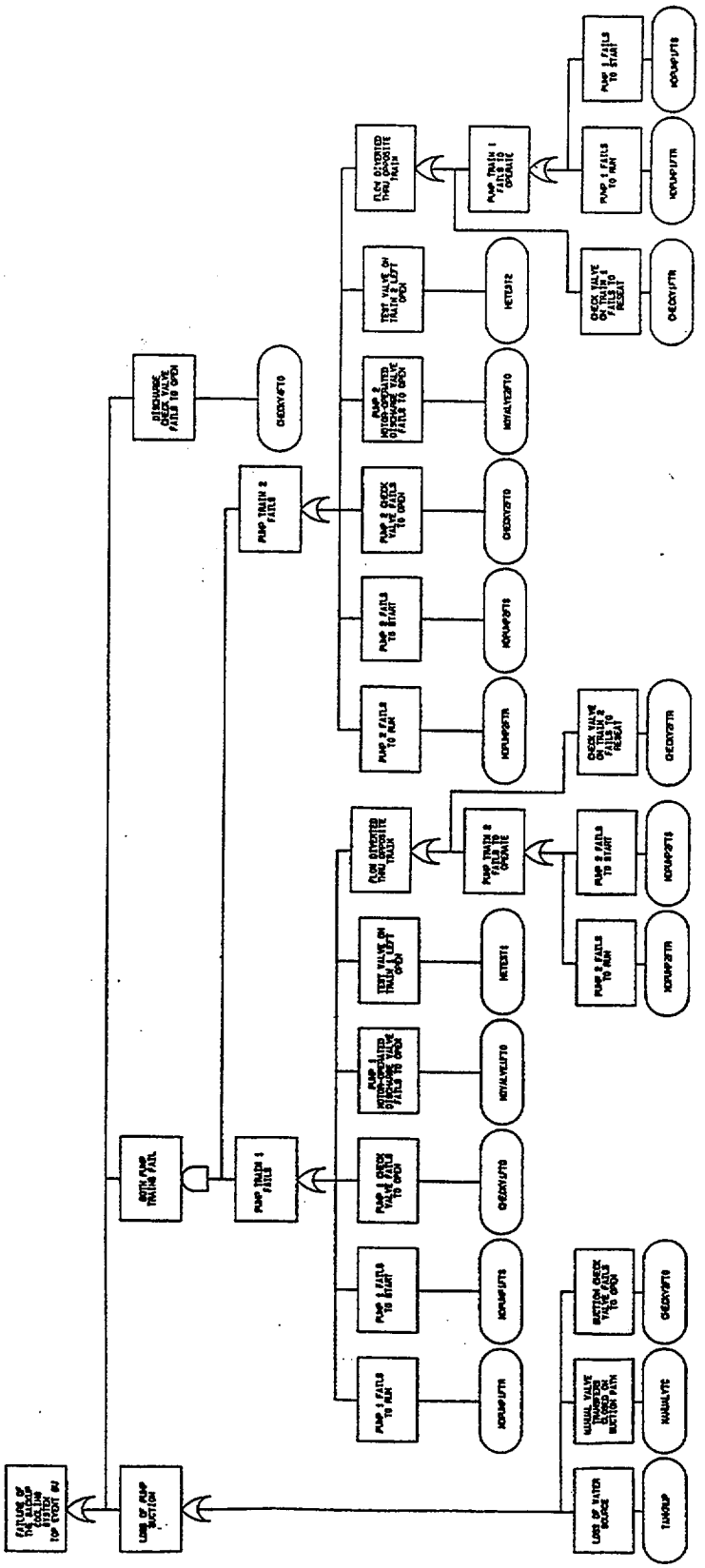


Figure 8.3 Example of fault tree for backup cooling system

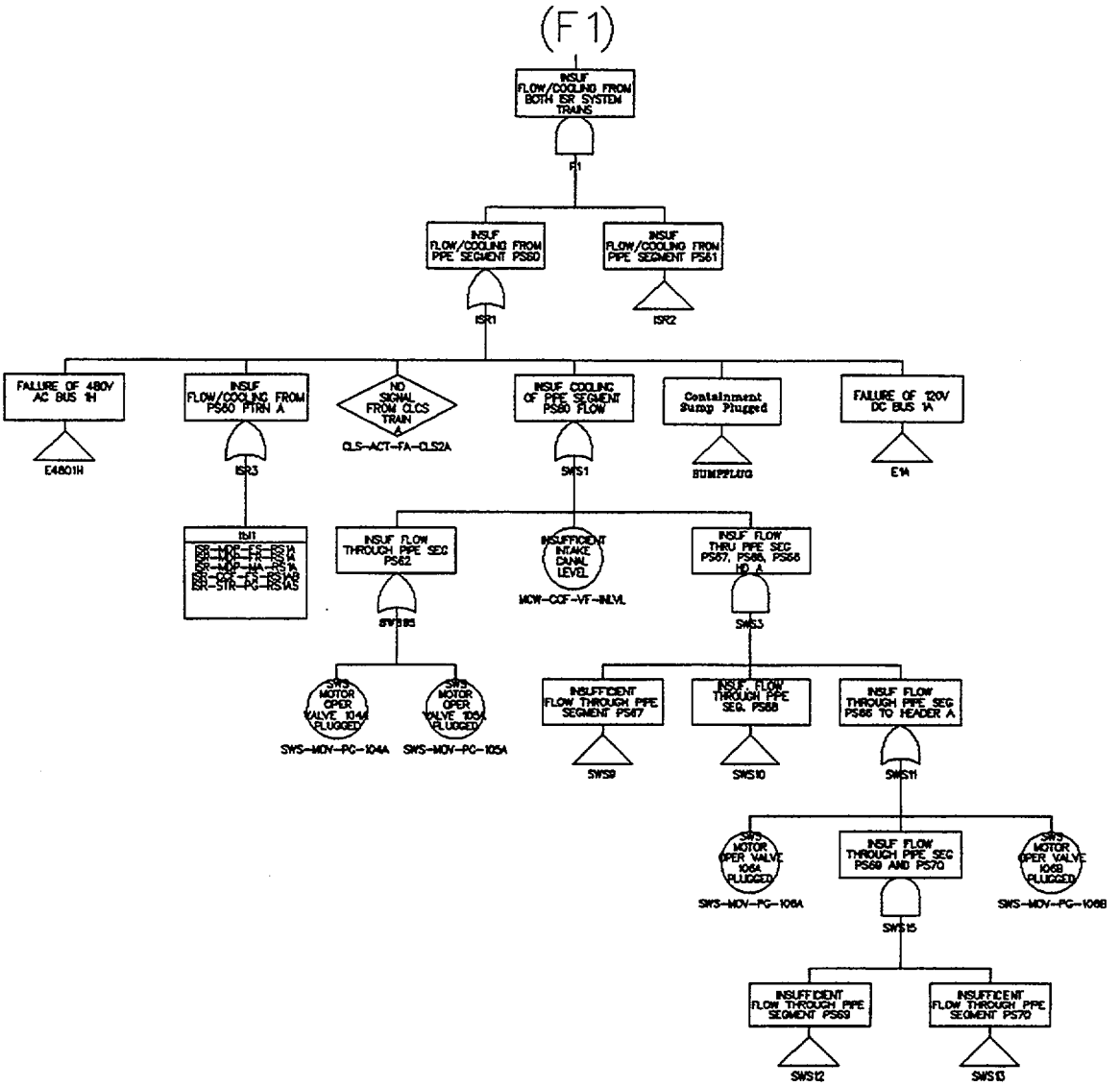


Figure 8.4 Example fault tree for inside spray recirculation

- for electrical power supply, at the buses from which components considered within the system are fed;
- for actuation signals, at the appropriate output cabinets of the actuation system; and
- for support systems providing various media (water, oil, air), at the main header line of the support system.

In cases where equipment or piping is shared between several systems, guidance to the proper establishment of the system boundary is usually provided by the system descriptions and drawings. Such cases must be brought to the attention of the system analysis task leader in order to avoid possible omissions and/or double counting of shared components.

6. It is important that a standardized format be used for coding the basic events in the fault trees. The formatting scheme should be compatible with the IRRAS code for the systems analysis, and the scheme should also enable the basic events to be clearly related to the following:

- component failure mode,
- specific component identification and type,
- specific system in which the component is located, and
- plant codings for the components.

To prepare the system models for either the concurrent or subsequent evaluation of environmental hazards, the system models should contain additional information on the location of the component and on the susceptibility of the component to the environmental hazard of interest (e.g., earthquake, fire, or flood). It is suggested that information of this type be encoded within the component name or provided on separate tables correlating events with applicable information.

To assist the analysis of dependent failures (other than those caused by extreme environments), the coding scheme should include information on location, designation of generic type, and test and maintenance procedures.

7. Fault trees should represent all possible failure modes that may contribute to the system's unavailability. This should include contributions due to outages of a system (or a portion of a system) for testing and maintenance. Human errors associated with failure to restore equipment to its operable state following testing and maintenance and human errors associated with accident response should also be included where applicable. Considerations of potential operator recovery actions are often specific to accident sequences and are best treated in the quantification of accident sequences (see Sections 11.1 and 11.2).

8. The following aspects of dependent failures should be reflected in the fault trees:

- interrelations between initiating events and system response,
- common support system faults affecting more than one front line system or component through functional dependencies,
- human errors associated with common test and maintenance activities, and
- components shared among frontline systems.

Dependent events should be modeled either explicitly or implicitly as noted in the following points:

- Multiple failure events for which a clear cause-effect relation can be identified should be explicitly

modeled in the system model. The root cause of these events should be included in the system fault tree so that no further special dependent failure model is necessary. This applies to multiple failures either caused by an internal equipment failure (such as cascade failures and functional unavailability events caused by components) or resulting from a clearly identifiable human error (such as human error in the steps of a prescribed procedure).

- Multiple failure events that are susceptible to dependencies, and for which no clear root cause event can be identified, can be modeled using implicit methods, such as the parametric models (see Section 8.2).

- There can be instances when there is a set of multiple failure events which explicit modeling of the cause is feasible (even in principle) but not performed because it would be too difficult. Encapsulating the events in a parametric model is the preferred approach. The decision is made by the analyst based on experience and judgment, taking into consideration the aim and scope of the analysis. In other cases, explicit modeling may be impracticable because the component failure data do not allow different failure causes to be distinguished. Explicit modeling should in principle go as far as reasonable, largely depending on the resources for the analysis and the level of detail required. Otherwise, an upper bound should be assessed and parametric modeling used. The analyst should clearly document the parametric modeling approach, the input, and the events that have been modeled explicitly.

9. The operability of some systems in response to an initiating event can be directly affected by the initiating event. Loss-of-coolant accident and loss-of-offsite power are two initiating events that can directly affect the performance of the responding systems. For these cases, the impact of the initiating event on the operability of each system should be explicitly included in each system fault tree. This representation also permits the proper quantification of the accident sequences. In the small event tree/large fault tree approach, which has been adopted in this study, the impact of the initiating events can occur at the component level.

10. To simplify and reduce the size of the fault trees, certain events are often excluded owing to their low probability in comparison with other events. Examples of simplifying assumptions are illustrated below:

    - Flow diversion paths for fluid systems should be considered only if they could seriously degrade or fail the system. A general rule is that the diversion path may be ignored for failure to start if the pipe diameter of the diversion path is less than one third of the primary flow path.

    - Spurious control faults for components after initial operation should only be considered if the component is expected to receive an additional signal to readjust or change its operating state during the accident.

    - Position faults prior to an accident are not included if the component receives an automatic signal to return to its operable state under accident conditions.

    Assumptions of this type must, of course, be documented and justified in the PRA report.

11. The testing procedures used in the plant must be closely examined to see whether implementation of the procedures can introduce potential failure modes. All potential failure modes identified must be documented. An example would be if, during testing, the flow path through a valve is isolated, and at the end of the test, the flow path remains closed (possibly due to human error) with no indication that the flow path is still closed.

12. Tripping of pumps and other safeguards, intended to protect a component, must be carefully identified since they can be a source of common mode failure. For example, spurious trips of auxiliary feedwater pumps on low suction pressure can lead to system failure if recovery does not occur.

13. In a sequence in which some systems succeed while others fail, it is important to make the system failures correctly conditional on the other systems' successes. Success trees are one way for expressing this conditional correspondence. There are certain advantages that are offered by algorithms which operate on the top event by simply deleting cutsets that violate the system success specified in the sequence.

Fault trees are to be used in the present analysis. Other methods have been used in PRAs. Selected issues, such as the determination of the frequency of an event initiated by the failure of a normally operating multiple train, may be best addressed by a method other than fault trees. For information purposes, two other methods are highlighted below.

8.1.3 Products

As identified in the task Documentation (Chapter 3), the current task will produce material for the final report. Specifically, the products for this task are a portion of the "Systems Analysis" appendix of the main report and the "Fault Tree" section of the backup documentation. In addition, this task is responsible for providing the system logic models in electronic form suitable for use in the sequence quantification activity.

8.2 Subtle Interactions

The objectives of this task are to identify and to explicitly model subtle interactions that could potentially cause single or multiple component failures, which are neither covered by a common cause failure analysis nor addressed in the dependency matrix. Ideally, most interactions would be caught in the system analyses, dependency matrices, and event tree models. This task would allow the analyst to systematically look for additional interactions that could have been missed in the earlier analyses.

8.2.1 Relation to Other Tasks

As indicated in Figure 8.1, the Subtle Interactions task has interactions with a number of other PRA tasks:

Plant Familiarization. This task obviously provides the basic information for possible interactions.

Quality Assurance and Documentation. The Subtle Interactions task has obvious interfaces with QA requirements and provides input to the PRA documentation.

PRA Scope. The systems of concern are those needed to perform the functions modeled in the PRA. For the Kalinin PRA, this means the system modeled for the full power operating state.

Initiating Event Analysis. The systems analysis can possibly identify additional initiating events related to a particular system.

Accident Sequence Development. The sequence development task needs to take subtle interactions into account.

System Modeling and Spatial Interactions. The Subtle Interactions task provides input to and receives feedback from these other two tasks of the Systems Analysis.

Quantification and Results. The Systems Analysis task must be completed before the quantification and results of the PRA are completed.

Fire, Flood, and Seismic Analyses. The effect of fire, flood, or seismic event scenarios on plant conditions and resulting subtle interactions need to be considered when these events are including in a PRA.

8.2.2 Task Activities

Subtle interactions are categorized as interactions between components and/or systems that can be caused by changes in the operating environment of the components, by conditions directly related to specific plant design and operational features or from the progression of a given accident sequence. These types of interactions mostly stem from mechanistic causes. If they could be identified a priori, then these interactions could be explicitly modeled in event trees or fault trees by using house events that would reflect the necessary causal relationships. Two examples that illustrate these types of interactions are provided below:

1. In a two-train, cross-tied system, failure of a discharge check valve (stuck open) could cause failure of the system. This can occur when one pump has been turned on while the pump in the other train has failed to start and run. In this case, the flow simply recirculates backward through the idle pump. This conditional interaction within a system would depend on a check valve failure in the cross-tie line and on the pump in the other train being idle. These types of mechanically determined interactions should be identified through detailed system evaluations and accounted for explicitly in system fault trees.

2. For certain types of motor-operated valve designs and for some systems where these motor-operated valve types are periodically tested using a low differential pressure (ΔP), there is little or no assurance that the valves would reliably operate when exposed to a high ΔP attributable to the progression of specific PRA scenarios. The unavailability of these motor-operated valves (both single and multiple) then would be dependent on the ΔP that is imposed by the accident sequence being analyzed. Appropriate house events should be used in the fault trees that explicitly consider the expected ΔP on valve operability for the scenarios being analyzed.

The above examples focused on hardware-oriented subtle interactions. There are also subtle human interactions that could cause multiple component failures. These types of human-caused subtle interactions are covered in the task Human Reliability Analysis (see Chapter 10).

The process by which these forms of subtle interactions are identified is not well structured. There are various information sources in the open literature that can be used for identifying these types of interactions. These sources include: past PRAs, historical events across the industry, and U.S. Nuclear Regulatory Commission (NRC) reports on industry-wide experiences. These documents are reviewed to see whether the interactions described are applicable for the specific PRA. Besides these sources of information for identifying potential plant-specific subtle interactions, the analysis should rely heavily on engineering judgment and in-depth system evaluations to assure that as many interactions as possible are identified and modeled. Notwithstanding, the guidance presented here and the state-of-the-art in PRA methodology do not provide any assurances that the list of identified interactions is complete and comprehensive. Furthermore, the lack of national and international databases documenting subtle interactions hinder future progress towards a comprehensive dependency analysis. Therefore, the extent to which these analyses are considered as complete would depend on the individual capabilities and combined experience of the PRA team. Assigning the occurrence probabilities to these subtle interactions would, however, be rather straightforward once the underlying mechanism for their occurrences is understood.

The following activities are normally performed as part of this task. However, it should be noted that U.S. practice in this area reflects embedded assumptions regarding U.S. plant design features and maintenance practices. Therefore, for the present application, the guidance provided for this task should be regarded only as a starting point. Development of a design-specific database on possible subtle interaction for different designs would be a positive step for future PRAs and augmentation of current PRAs.

8.2.2.1 Activity 1 - Review of Literature

The appropriate literature is reviewed and the current understanding of any subtle interactions that are considered applicable to the Kalinin plant is documented. The focus of the literature review deals with information gleaned from past PRAs and reports documenting their insights, various safety studies, generic issues, etc. For example, NUREG/CR-4550 (Ericson, 1990) contains anecdotal information on some of the experiences with subtle interactions found in U.S. plants. There could be other, more relevant information sources. A starting point, for example, could be the insights found in current or recent PRA studies for other VVER plants as those found in the IAEA document WWER-SC-152 (IAEA, 1996).

8.2.2.2 Activity 2 - Cataloging Subtle Interactions

The current understanding of the subtle interactions, based on major historical events and other formalized studies, is catalogued in a manner suitable for data analysis. Summary of generic issues, issues identified in annual reports (such as NRC, 1996) published by the NRC Office of Analysis and Evaluation of Operational Data, annual reports (NRC, 1986) generated by the Accident Sequence Precursor Studies Program, and NRC notices are some of the documents typically reviewed. Interviews with plant staff could also be quite useful in this case.

8.2.2.3 Activity 3 - Engineering Evaluations

Engineering evaluations are performed by selecting a group of components that have a common characteristic–for example, same location, same actuation logic, etc. The engineering evaluation could be a set of "what if" questions that examine the conditions imposed by various scenarios on the system and the performance of components within the system. These engineering evaluations should be performed with the help of plant staff who may already suspect or be aware of these types of plant-specific interactions.

8.2.2.4 Activity 4 - Documentation

Any subtle interactions considered relevant to the PRA are documented. One or more ways in which the plant logic models (fault trees and event trees) can be augmented are proposed that will appropriately account for the mechanistic processes involved with these interactions. Ways for estimating the probabilities for such occurrences are also proposed and, wherever possible, estimates are provided. These documents should also be distributed to both the system and event tree analysts to assure consistency in approach and completeness in meeting task objectives.

8.2.3 Products

The only product for this task would be a detailed descriptions of the applicable subtle interactions that have been identified, the sources of information used, and the guidance as to how these interactions should be modeled within the Kalinin PRA logic models.

8.3 Spatial Interactions

The objective of this task is to identify potential environmental hazard scenarios at the plant. This objective is accomplished by systematically identifying hazard sources and potentially vulnerable plant equipment. Hazard scenarios are postulated from the hazard and plant equipment location information developed in this task. This task also includes a screening of the postulated hazard scenarios. The scenarios that survive the screening process constitute one of the key inputs to the subsequent detailed fire analysis (see Chapter 12) and flood analysis (see Chapter 13). The equipment location information is also used to support the assessment of seismic events (see Chapter 14).

The external events of interest in a PRA can be generally grouped into two categories: events that are truly external to the plant (e.g., seismic events or severe meteorological phenomena) and events that involve internal hazards (e.g., fires and floods) that can simultaneously affect nominally separated components. The term "environmental hazards" is used to describe the latter. The primary thrust of the spatial interactions analysis is to provide a first iteration of the identification and quantification of potential environmental hazard scenarios. However, the information developed in the spatial interactions

task also supports the analysis of external events, such as seismic events through the identification of the spatial relationships of plant components.

8.3.1 Relation to Other Tasks

As indicated in Figure 8.1, the Spatial Interactions task has some interactions with other PRA tasks, especially those involving fire, flood, and seismic events:

Plant Familiarization. This task obviously provides the starting point for spatial interactions considerations.

Quality Assurance and Documentation. The Spatial Interactions task has obvious interfaces with QA requirements and provides input to the PRA documentation.

PRA Scope. The systems of concern are those needed to perform the functions modeled in the PRA. For the Kalinin PRA, this means the system modeled for the full power operating state.

Initiating Event Analysis. Knowledge of the initiating events is needed for the development of potential hazard scenarios involving spatial interactions.

Accident Sequence Development. The sequence development task needs to account for the spatial interactions identified.

Subtle Interactions and System Modeling. The System Modeling task provides input to and receives feedback from these other two tasks of the Systems Analysis.

Quantification and Results. The Systems Analysis task must be completed before the quantification and results of the PRA are completed.

Fire, Flood, and Seismic Analyses. The completion of the Spatial Interaction task is essential before proceeding with the fire and flood analysis. Spatial relationships of plant equipment is also essential for the seismic analysis.

8.3.2 Task Activities

It should be recognized that much of this task involves the use of expert knowledge, engineering judgment, and knowledge of the internal events PRA. During the conduct of this task, it is assumed that the internal events plant model is sufficiently mature so that conservative but defensible screening of scenarios can be accomplished. It is unlikely that a "final" plant model will be available when this task is being performed. Therefore, any plant model changes made after the scenario screening process has been performed should be reviewed to determine if the results of the screening process are affected.

The analytical approach outlined in this procedure guide is the result of an evolving process. One early attempt to formally address the hazards associated with the spatial relationships of equipment in a plant was performed as part of the Seabrook Probabilistic Safety Assessment (PLG, 1983). The approach has been utilized in many subsequent PRAs, such as the assessment of environmental hazards at Brookhaven National Laboratory's High Flux Beam Reactor (Ho and Johnson, 1994) and in the Gösgen Probabilistic Safety Assessment (PLG, 1994). The methodology outlined here begins by first identifying the sources of hazards and constructing scenarios arising from those hazards. An alternative methodology can be constructed that is "target" based rather than "source" based. The two approaches are conceptually similar. Both involve a systematic scrutiny of the plant to identify hazards and the development of scenarios. The target-oriented approach was chosen for the NUREG-1150 analyses (Bohn and Lambright, 1990). An example of the application of this approach can be found in Bohn et al. (1990).

This task is accomplished by completing five activities:

1. Collection of plant information and performance of a plant walkdown,
2. Development of a spatial interaction database,
3. Identification of potential hazard scenarios,
4. Performance of a preliminary screening of the identified scenarios, and
5. Development of scenario tables.

Each of these activities is discussed below.

8.3.2.1 Activity 1 — Collection of Plant Information and Performance of a Plant Walkdown

The spatial interactions analysis starts by collecting and organizing all of the relevant plant information. This includes a review of the plant general arrangement and technical drawings to collect information about the plant layout, equipment locations, functions of the equipment, and potential hazard sources. The PRA dependency matrices, system analyses, and event models are also desirable sources of information to help the spatial interactions analysts become knowledgeable about the plant systems, intersystem dependencies, the initiating events, and the plant response to the initiating events.

A plant walkdown checklist is developed to help the spatial interactions analysts systematically itemize the information collected during the plant walkdown and for documenting questions that must be resolved.

A typical checklist for one zone of the plant would contain the zone ID and name, the building name, the PRA and non-PRA systems and/or trains, any large heat, smoke, or water sources as well as other sources and their locations. For the PRA and non-PRA equipment, the vulnerabilities and hazard sources would be listed. Component separation would be indicated, and photographs or sketches attached. For each hazard source, information regarding location, detection, suppression, access, occupancy, and traffic in the area would be provided.

Specific hazards and hazard sources are listed in the discussion of Activity 2. It should be noted that these checklists serve primarily as "notebooks" for the analysts, whereas formal documentation of the information is made through the databases and scenario tables discussed below. In most cases, it is not necessary to complete the entire checklist for a specific location, and a single checklist may be used to document several similar locations.

To prepare for the plant walkdown, a systematic scheme to identify locations within the plant is required. As indicated below (in the discussion of Activity 4), it is desirable that, at least initially, broad physical boundaries be used to define plant locations. These locations may be based on physical considerations, such as walls and doors, or on physical separation distances. In general, it is desirable to define larger zones in buildings, such as the turbine or off-gas buildings, and smaller zones in buildings, such as the auxiliary building, the control building, or within containment. Existing information, such as the definition of fire areas or flood zones, may be a useful starting point. The areas or zones defined at this point will be refined and revised as the analysis continues (i.e., in the fire and flood analyses). Many areas will likely be shown to be risk insignificant in the subsequent screening process. Other areas will be of interest only if the hazard propagates to adjoining areas. Still, other areas will require subdivision in order to appropriately describe the risk scenarios. The important point is that a systematic scheme is required at this time that will address all locations in the plant.

A plant walkdown is conducted to confirm and augment the information gathered from the documents, to inspect the amount and location of possible transient hazards, and to help visualize the spatial interactions of hazards with equipment. Photographs, sketches, and notes are often made to document complex configurations. The plant walkdown team is responsible for identifying all potential hazard sources and the location of equipment of interest throughout the plant. The equipment of interest is equipment whose failure or degraded function would lead to a plant transient, reactor runback or trip, or turbine runback or trip. It also includes equipment that has a role in defining the progression of events following these types of upset conditions. For convenience, we refer to such equipment as PRA-related equipment, or more succinctly, "PRA equipment." The team also evaluates the routing of important electrical power, control and instrument cables, and system piping. It is important that every plant location be systematically examined to ensure completeness of the analysis.

8.3.2.2 Activity 2 — Development of Spatial Interaction Database

The information and results from these walkdowns are sorted and catalogued to ensure consistency and traceability throughout the analysis. Databases are then developed to

minimize the potential for errors and to enhance the flexibility for data retrieval and searches. It is anticipated that existing database software is adequate. These databases contain the following information:

- Identification of locations within the facility
- Location of all PRA equipment and related cables and piping
- Susceptibility of equipment, cables, and piping to hazards
- Hazard mitigation features
- Hazards associated with equipment, cables, and piping
- Location of all hazards
- Potential hazard propagation pathways between locations
- PRA top events that include the affected equipment.

These databases are cross linked so that one can identify, for example, the PRA equipment, the hazards, and the mitigating features for any given location.

The specific PRA-related equipment of interest are those components (and their cables) whose failure, or change of status, may cause an initiating event or may impair the availability of systems required for accident prevention and mitigation. These components are identified by a thorough review of the PRA event and system models. Passive components, such as check valves, are not normally susceptible to fire or other environmental hazards but are included in the list to support the seismic analysis. Other passive components, such as manual valves and hoses, are of particular interest if plant operators are required to manipulate this equipment as part of their emergency response actions. These actions by the operator may be hindered if a hazard (such as a fire) is present where this equipment is located. The equipment database also includes power, control, and instrumentation cables that support normal and emergency operation of the PRA components.

The types of hazards considered in the spatial interactions analysis include:

- Fire and smoke
- Explosion
- Flood water
- Water spray
- Steam spray
- Missiles
- Falling objects
- Chemical hazards.

Equipment in a large complex facility is generally exposed to a variety of hazards. The components in different systems are susceptible to different specific hazards, based on the characteristics of the components, their location, and the types of protection features that are available. For example, electrical cables may be susceptible to damage by a fire, causing loss of power to equipment or generating spurious signals to instrumentation and control equipment. They are not generally susceptible to damage if they are submerged by a transient flood, unless electrical contacts are exposed. Table 8-1 lists general types of equipment that are susceptible to damage if a particular hazard occurs in their location. Table 8-2 lists typical hazards that may be created by a variety of components. The identification of specific hazards in each location will provide the basis for later quantification of the hazard scenarios. Typically, the following categories of plant components are considered as possible ignition sources for nuclear power plant fires:

- Batteries
- Battery chargers
- Cabinets (including logic cabinets, relays, panels, fuses and switches)
- Cables (including control and power cables)
- Control room equipment
- Diesel generators
- Generators
- Heating, ventilation, and air conditioning equipment
- Motor-operated valves
- Motor control centers
- Pumps and chiller units
- Air compressors
- Switchgear
- Turbines
- Large transformers
- Small transformers
- Transient material.

Table 8-1 Equipment hazard susceptibility

Hazard Type	Hazard Description	Equipment Susceptible to Damage in the Designated Area
CA	Chemical Hazards	All active components; electrical parts of equipment.
EX	Explosion	All equipment and components.
FO	Falling Objects	All equipment and components in the pathway.
FS	Fire and Smoke	All active components; electrical parts of equipment.
FW	Flood Water	All active components that are not waterproof and all electrical parts of equipment (not including cables) below water level.
MI	Missiles	All equipment.
SS	Steam Spray	All active components that are not waterproof and all electrical components except for cables.
SW	Water Spray	All active components that are not waterproof and all electrical components except for cables.

Table 8-2 Hazards associated with equipment

Description	Associated Hazards*
Air Compressor	MI, FS
Air Handling Unit	FS, FW, SW
Air-Operated Valve	
Battery	FS, EX
Battery Charger	FS
Caustic Piping	CA
Caustic Storage Tank	CA
Chiller	MI, SS, FW, SW
Concrete Coating	FS
Control Cable	FS
Crane	FO
Distribution Panel	FS
Electric Heater	FS
Electrical Cabinet	FS
Fan	FS, MI
Filter	FS
Fire Hoses	FS, SW
Flammable Gas	EX, FS
Heat Exchanger/Cooler	FW, SW
Heater; e.g., space	FS
Motor Control Center	FS
Motor-Driven Pump	FS, MI
Motor-Operated Valve	FS
Oil System; e.g., pump or lube	FS, EX
Pneumatic Valve	
Portable Extinguisher (CO_2)	MI
Portable Extinguisher (Water)	MI, SW
Power Cable	FS
Pressurized Canisters	MI
Propane Generator	MI, EX, FS
Radiation Monitor	
Relay Cabinets	FS
Solenoid Valve	FS
Sprinklers, Dry Pipe	FW, SW
Steam Piping	SS
Switchgear	FS
Transformer	FS, EX
Transient Fuel	FS
Water Piping	FW, SW
Water Tank	FW, SW
*Defined in Table 8-1	

For internal floods, the following specific sources are sought and documented:

- Valves
- Piping
- Tanks
- Heat exchangers
- Drains
- Heating, ventilation, and air conditioning ductwork.

It is also desirable to know the nominal pressure of some components.

The next activity of the analysis uses the equipment/location databases to correlate the sources of specific hazards with the locations of PRA components that are susceptible to damage from those hazards.

8.3.2.3 Activity 3 — Identification of Potential Hazard Scenarios

The spatial interactions databases are analyzed to sort and categorize types and sources of potential hazards in each plant location. Special attention is focused on all locations that contain PRA equipment. However, locations that do not contain PRA equipment are also examined if they contain hazards that may propagate to other locations containing PRA equipment, e.g., flood water that drains from upper floors to lower elevations in a building or causes barrier failure. This activity defines the scope of the hazard scenarios developed for each plant location.

8.3.2.4 Activity 4 — Perform Preliminary Screening

It is often possible to eliminate a large number of locations and hazards from further analysis, based on a qualitative examination of the information from the preceding activities. This preliminary screening analysis considers the following possible impacts for each location from each potential hazard.

1. The hazard and the propagation of the hazard do not cause an initiating event (e.g., a reactor trip or a runback demand) and concurrently do not damage any PRA equipment.
2. The hazard may cause an initiating event, but it does not damage any PRA equipment.
3. The hazard may cause an initiating event, and it may damage equipment in one or more systems modeled in the PRA.
4. The hazard does not cause an initiating event, but it may damage equipment in one system modeled in the PRA.
5. The hazard does not cause an initiating event, but it may damage equipment in more than one system modeled in the PRA.

All locations and hazards that satisfy the first screening criterion (does not cause an initiating event and does not damage PRA equipment) are eliminated from further consideration in the analysis. Within the context defined by the PRA models, these hazards have no measurable impact on plant risk.

Locations and hazards that may cause an initiating event but do not damage PRA equipment (the second criterion) are examined more carefully to determine the type of initiating event that can occur. If the initiating event has been evaluated as part of the internal events analyses (e.g., reactor trip, loss of feedwater, etc.), no additional analysis is necessary to separately quantify the contribution to plant risk by the external event. The internal initiating event frequency data already account for the contributions from all observed causes, external and otherwise. However, if the hazard can cause an initiating event that has not yet been considered, the location is retained for more detailed analysis in this portion of the study.

A similar screening approach is used for hazards that satisfy the fourth criterion (does not cause an initiating event but may damage equipment in one PRA system). If the hazard can cause equipment failures that are already included in the system fault tree models and equipment reliability databases, no additional analysis is necessary to separately evaluate these causes for system unavailability. However, if the hazard can cause unique failure modes or introduce dependencies that are not otherwise evaluated in the system

fault trees, the location is retained for more detailed analysis in this portion of the study.

All hazards that satisfy the third and fifth screening criteria (the hazards can either cause an initiating event and impart damage to at least one PRA system or it may cause damage to multiple PRA systems, respectively) are retained for the final activity of the spatial interactions analysis.

At this point in the analysis, preliminary screening is based only on the qualitative criteria summarized above. No quantitative information or comparative numerical analyses are applied to eliminate locations or hazards from further consideration. If there is any question about the applicability of a particular screening criterion, the hazard or location in question is retained for more detailed analysis in the subsequent activities. Thus, these preliminary screening criteria may be applied consistently without the need to reexamine these hazards or locations, even if the numerical results from the risk models are later refined.

The locations that remain after this preliminary screening process are often called "critical locations" or "functional impact locations." These locations are defined by a combination of the type of hazard being examined, the physical plant layout, the types of equipment in each plant area, and the functional impacts that may occur in the PRA models if the affected equipment is damaged. It is desirable to initially define rather broad physical boundaries for each location. This provides a manageable number of different locations that must be examined in the more detailed activities of the analysis. However, the locations must also be defined consistently with respect to the possible PRA impacts from each hazard scenario. Thus, a particular functional impact location may include a single room, part of a room, or a combination of plant areas, and more than one hazard scenario may be developed for each location. A unique designator is assigned to each functional impact location to facilitate its identification in later phases of the analysis.

8.3.2.5 Activity 5 — Development of Scenario Tables

Hazard scenarios are developed for each hazard and each functional impact location that survives the preliminary screening process. Each hazard scenario is defined by an impact, or set of impacts, that may develop if a postulated hazard occurs within the location. In the full context of the PRA models, a complete scenario always represents a class of events that may occur in real plant experience. For example, a complete fire scenario includes an ignition phase, propagation, detection, suppression, damage to PRA equipment, and the subsequent sequence of equipment responses and operator actions that result in either safe plant shutdown or core damage. However, at this activity in the analysis process, each hazard scenario is limited to identification of the hazard source and documentation of the PRA equipment that may be affected directly by that hazard.

To ensure completeness in the more detailed analyses performed in later activities, the hazard scenarios are typically defined at a rather general level and are all encompassing. For example, a fire scenario is defined as "localized" when any fire event that may occur within the functional impact location does not have any adverse impact on adjacent locations. This fire scenario actually represents a large class of possible fire events that range from very small fires that may damage only one component to a major fire that may damage all equipment in the location.

In the spatial interactions analysis, a scenario always assumes that the identified hazard damages all of the PRA equipment in the location, regardless of the size, severity, or duration of the hazard event. This is obviously a very conservative assumption for many actual hazards. For example, a small fire in a corner of a large room may not damage any equipment a few meters from the ignition point. However, the application of very conservative assumptions is acceptable and desirable in this phase of the analysis. This keeps the number of individual scenarios within a practically manageable limit, and it facilitates an efficient screening process to ensure that no potentially important scenarios are overlooked.

In practice, the first pass through a quantitative screening analysis (as described in Chapters 12 and 13) typically demonstrates that a large number of these conservatively defined scenarios are clearly insignificant contributors to plant risk. These scenarios are documented and are removed from further detailed consideration. A relatively small number of scenarios may not be eliminated during the first application of quantitative screening. For these scenarios, this activity of the analysis process marks the point at which successive refinements are applied to redefine the scenario, to reexamine its impacts, and to develop more realistic models for its actual contribution to risk.

A unique designator is assigned to each hazard scenario. These designators are later used in the PRA event models to identify each internal hazard initiating event. The functional impact location designators are not used to identify the scenarios because more than one scenario may be developed for a particular location, e.g., a fire that causes open circuits, a fire that causes short circuits, a flood, etc. Each scenario is then documented in a scenario table.

If propagation of the hazard scenario is possible between locations (e.g., flood water originates in location A and propagates to location B), then a separate unique scenario is defined and a separate scenario is constructed.

Table 8-3 illustrates a typical scenario table. In this illustration, each scenario table has a 5-item header followed by nine data entries. The header describes the location of the scenario. The location description includes the building, the physical areas included in the scenario, a short description of the location, and the unique designator for the functional impact location. In the example from Table 8-3, the functional impact location includes only Room E-0251. This room is the Division 1 switchgear room at Elevation 0.0 m of the electrical building. This location has been assigned the functional impact location designator S1. However, a single functional impact location may also include a large number of physical areas in the plant.

The last header item is the scenario designator. It is often helpful to assign designators that easily identify both the particular type of hazard being evaluated and the functional impact location. For example, designator FIRES1 applies to a fire event scenario in electrical building location S1. This is especially useful if more than one scenario is developed for a particular location.

The following nine data entries are included in each scenario table. Entries 1 through 5 and 7 (partial) are completed within this task's activities. Entries 6, 7 (partial), 8, and 9 are completed during the detailed scenario analysis phase (i.e., the fire and flood analyses).

1. Type of Hazard Source. This entry documents the hazard sources identified during the initial review of plant information and the plant walkdown. The major fire hazard sources in the switchgear room, for example, should include the switchgear, electrical cables, and small quantities of transient combustibles that may be brought into the room during maintenance activities.

2. Scenario Initiation. This entry identifies the specific type of hazard. For scenario FIRES1, the hazard is a fire.

3. Path of Propagation. The path for possible propagation of the hazard to other locations is listed in this entry. A hazard is designated as localized if it does not propagate to other locations. As noted previously, most functional impact locations are defined very broadly to encompass all possible hazard scenarios within the location and to avoid a significant possibility of propagation between locations. Therefore, according to this practice, most hazards are designated as localized within the defined location. Scenario FIRES1 evaluates a fire confined within the switchgear room.

4. Scenario Description. This entry provides a brief description of the scenario.

Table 8-3 Illustration of a typical scenario table

BUILDING		E
LOCATION		E-0251
LOCATION NAME		Division 1 Switchgear Room, Elevation 0.0 m
LOCATION DESIGNATOR		S1
SCENARIO DESIGNATOR		FIRES1
1.	TYPE OF HAZARD SOURCE	Switchgear, Cables, Transients
2.	SCENARIO INITIATION	Fire from any hazard source in Item 1
3.	PATH OF PROPAGATION	
	A. PATH TYPE	None (localized)
	B. PROPAGATE TO	None
4.	SCENARIO DESCRIPTION	Fire damages Division 1 switchgear
5.	HAZARD MITIGATION FEATURES	Detectors
6.	SCENARIO FREQUENCY	3.96×10^{-3} per year
7.	PRA-RELEVANT EQUIPMENT WITHIN THE AREA	

Equipment	Top Event	Equipment Impact
BS1-EP	EP	Note 1
BS1-BA	BA	Note 1
BS1-CA	BA	Note 1
BS1-CJ	BA	Note 1
BS1-BU	BU	Note 1
BS1-EU	BU	Note 1
BS1-FU	BU	Note 1

8.	RETAINED AFTER SCREENING ANALYSIS	No
9.	NOTES	
	1. It is assumed that any fire in this area affects the power supplies for all equipment powered from 10 kV bus BA, 6 kV bus BU, and 380 V AC bus EP. The split fraction rules for Top Events BA, BU, and EP have been modified to fail power from these buses for all fires in this area.	

5. Hazard Mitigation Features. This entry briefly summarizes the hazard mitigation features that are present in the location. Table 8-4 provides a list of typical mitigation features for different types of hazards. The scenario tables generally summarize only automatic detection, automatic suppression, and passive mitigation features. Possible manual mitigation features are not generally listed in these tables. Thus, Table 8-3 notes that the switchgear room contains fire detectors, but it does not identify the availability of manual fire suppression equipment. The effectiveness of these mitigation features is not evaluated quantitatively during the initial scenario screening process. More information may be provided about mitigation features for scenarios that require detailed quantitative analyses of hazard initiation, growth, propagation, detection, and mitigation.

6. Scenario Frequency. This entry lists the mean annual frequency at which the hazard is expected to occur. This frequency is equivalent to the initiating event frequency for the hazard scenario. It is the total frequency for any hazard type being evaluated, regardless of the hazard severity. Thus, Table 8-3 indicates that the mean frequency for switchgear room fires of any reportable size is approximately 3.96×10^{-3} fire per room-year, i.e., one fire is expected to occur in Room E-0251 every 253 years. Although this factor is listed in Table 8-3, the hazard occurrence frequency is actually assessed during the second phase of the internal plant hazard analysis. The frequency assessment process is described in Chapters 12 and 13.

7. PRA Equipment within the Area. This entry lists all PRA equipment in the location. This list is derived from the spatial interactions equipment location databases developed in Activity 2 of the analysis. This entry also identifies the PRA event tree top event for each component, and it briefly summarizes the functional impacts assumed to occur if the equipment is damaged by the hazard.

8. Retained after Screening Analysis. The quantitative screening process is described in later tasks (see Chapters 12 and 13). This entry documents whether the potential risk significance of the scenario is small enough to justify its elimination from further detailed analysis.

9. Notes. This entry includes additional detailed notes that document specific information about the hazard frequency assessment and the functional impact analysis.

A scenario table is developed for every hazard scenario that is retained from the preliminary qualitative screening process in Activity 4 of this task. Each table completely describes the defined scenario, the occurrence frequency of the scenario, and its specific impacts in the PRA models.

8.3.2.6 Additional Guidance

The risk analysis of environmental hazards is conducted in at least two stages. The first stage, scenario development, begins with the identification of potential environmental hazards at a broad level and ends with an extensive list of hazard scenarios at each location within the plant that could be potentially significant to risk. This first stage is referred to as a spatial interactions analysis and is the focus of this task. The second stage, the subject of the fire and flood analyses, performs detailed analyses to determine the plant impact frequency, evaluates plant recovery actions, and assesses the risk significance of the scenarios. Initially, for screening purposes, the scenario risk analysis applies conservative estimates for the occurrence frequency assessment and plant impact. Upon focusing on the important scenarios that are retained after screening, the analysis increases the level of detail considered reducing the conservatism in the original treatment of those scenarios and requantifying the impact to risk.

Table 8-4 Typical hazard mitigation types

Mitigation Type	Hazard Types*
Curb	FW
Drain	FW
Drain Pump	FW
Fire Damper	FS
Fire Detector (Thermal)	FS
Fire Hoses	FS
Missile Shield	MI
Watertight Door (Blockage)	FW
Nonwatertight Door (Drainage)	FW
Pedestals	FW
Portable Extinguisher (CO_2)	FS
Portable Extinguisher (Dry Chemical)	FS
Portable Extinguisher (Other)	FS
Radiant Energy Heat Shields	FS
Sprinklers (Preaction)	FS
Standpipe	FS
Sump	CA, FW
Sump Pump	CA, FW
Sump or Room Flood Alarm	FW
Walls (1½-Hour Rates)	FS
Walls (Other)	FS
Yard Fire Hydrant	FS
*As defined in Table 8-1.	

The processes in the overall environmental hazards risk analysis are inherently counteractive and must be balanced in a meaningful practical risk analysis. Ideally, the spatial interactions analysis identifies all potential hazard scenarios regardless of occurrence frequency or potential degree of impact on the plant that can cause any conceivable amount of damage. This would ensure that all locations and all possible hazards will be fully examined. On the other hand, to use available resources most efficiently and to maintain a proper balance throughout the risk assessment process, the detailed scenario risk analysis demands that only relatively risk-significant scenarios be evaluated in detail. This "top-down" approach to risk assessment minimizes the effort in quantifying the risk associated with unimportant locations. Therefore, the scenarios identified during the spatial interactions analysis are to be as comprehensive as possible while maintaining a manageable number for the subsequent detailed fire and flood analyses. In practice, experience has shown that the two stages of the analysis of environmental hazards are somewhat iterative and must be closely coordinated.

8.3.3 Products

During the conduct of this task, the following will be developed: a scheme for describing plant locations, a form specialized for the plant to assist in the documentation of the plant walkdown, a set of completed walkdown forms, and an information database that describes the location of hazards as well as plant equipment of interest.

As identified in the task Documentation, the current task will produce draft material for the final report. Specifically, a draft portion of the "Spatial Interactions" appendix of the main report will be developed that will include a description of the methodology used to identify and screen hazard scenarios and the information derived by the

analysis. The information derived includes the identification and characterization of plant hazards, the location and relative apportionment of plant equipment according to location, and tables describing the potential hazard scenarios

8.4 References

Bohn, M. P., et al., "Analysis of Core Damage Frequency: Surry Power Station, Unit 1, External Events," NUREG/CR-4550, Vol. 3, Rev. 1, Part 3, Sandia National Laboratories, December 1990.

Bohn, M. P., and J. A. Lambright, "Procedures for the External Event Core Damage Frequency Analyses for NUREG-1150," NUREG/CR-4840, Sandia National Laboratories, November 1990.

Chu, T.-L., et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1," Vol. 2, NUREG/CR-6144, Brookhaven National Laboratory, June 1994.

Drouin, M., et al., "Analysis of Core Damage Frequency from Internal Events: Methodology Guidelines," NUREG/CR-4550, Volume 1, September 1987.

Ericson, D. M., et al., "Analysis of Core Damage Frequency: Internal Events Methodology," NUREG/CR-4550, Vol. 1, Rev. 1, Sandia National Laboratories, January 1990.

Haasl, D. F., et al., "Fault Tree Handbook," NUREG-0492, U.S. Nuclear Regulatory Commission, January 1981.

Ho, V. S., and D. H. Johnson, "Probabilistic Risk Analysis of Environmental Hazards at the High Flux Beam Reactor," Final Report, PLG-0975, prepared for Brookhaven National Laboratory, PLG, Inc., April 1994.

IAEA, "Insights from PSA Results on the Programmes for Safety Upgrading of WWER NPPs," WWER-SC-152, 1996-11-29, limited distribution, International Atomic Energy Agency, October 1996.

NRC, "The Use of PRA in Risk-Informed Applications," NUREG-1602, Draft Report for Comment, June 1997.

NRC, "Analysis and Evaluation of Operational Data-Annual Report, 1994-FY-95," NUREG-1272, Vol. 9, No. 1, U.S. Nuclear Regulatory Commission, July 1996.

NRC, "Precursors to Potential Severe Core Damage Accidents: A Status Report," NUREG/CR-4674, U.S. Nuclear Regulatory Commission, issued periodically (annually) since 1986.

PLG, "Gösgen Probabilistic Safety Assessment," prepared for Kernkraftwerk Gösgen-Däniken AG, PLG-0870, PLG, Inc., February 1994.

PLG, "Seabrook Station Probabilistic Safety Assessment," PLG-300, prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company, PLG, Inc., December 1983.

9. DATA ANALYSIS

Data analysis is a key component of the third element in a Level 1 probabilistic risk assessment (PRA) (refer to Figure 1.3). Data analysis consists of three interrelated tasks--namely, determining (1) the frequency of initiating events, (2) component reliability, and (3) common-cause failure probabilities. This is shown on the flowchart in Figure 9.1. The first of these tasks quantifies the frequency of each group of initiating events identified in the task Initiating Event Analysis (refer to Chapter 6). The second task is to obtain plant-specific estimates of the unavailability of specific equipment. The third task is to determine the final values to be used in the parametric models of common-cause failures. Figure 9.1 shows the important relations between the tasks under data analysis and the other major components of the PRA. These relationships are explored in more detail in each of the section describing describing the three tasks. Frequency of Initiating Events is discussed in Section 9.1, Component Reliability in Section 9.2, and Common-Cause Failure Probabilities in Section 9.3.

9.1 Frequency of Initiating Events

The objective of this task is to quantify the current frequency of each group of initiating events identified in the task Initiating Event Analysis (Chapter 6). It is desired that the frequencies be expressed in the form of uncertainty distributions and that the determination of the frequencies take advantage of all relevant evidence.

9.1.1 Relation to Other Tasks

The present task requires input from Initiating Event Analysis (Chapter 6) and provides output necessary for the Initial and Final Quantification of Accident Sequences (Chapter 11). A more subtle interface is found with the task System Modeling (Section 8.1). System logic models may be necessary to quantify specific initiators, such as loss of a support system.

The grouping of the individual initiators based on the expected plant response is performed as part of the task Initiating Event Analysis. Each group

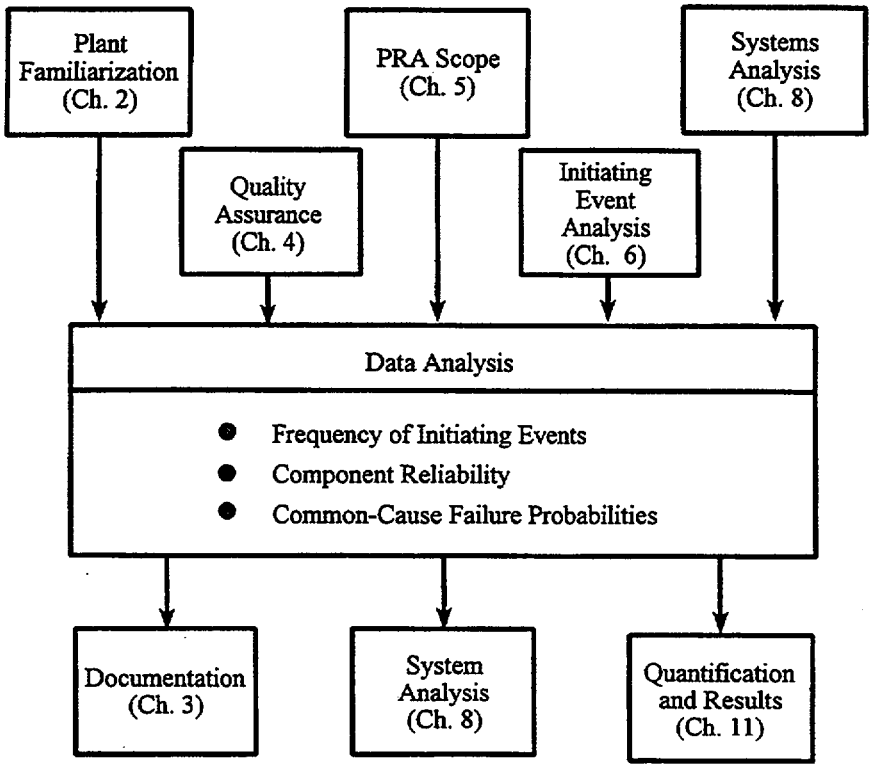


Figure 9.1 Relationships between data analysis and other tasks

includes a number of initiators that have similar responses for the plant systems and operators. It is important that the understanding of the rationale used in the grouping process be carried over to the present task.

9.1.2 Task Activities

The goal of this task is to develop a probabilistic description of the frequency of the initiating events of interest along with supporting documentation. From the point of view of expressing the frequency of initiating events at a specific plant, the ideal situation would be if sufficient experience was available from that plant to fulfill all the data analysis needs. The nature of the events of interest, however, prevents this from being the case (and from the point of view of plant performance and safety, the occurrence of such events is undesirable). Many events of interest (e.g., large loss-of-coolant accidents [LOCAs]) are not expected to occur during the life of the plant. Therefore, additional sources (experience from identical or similar plants and expert knowledge) are needed for acquiring supplemental information. This additional information is merged in such a way that the combined distribution of plant-specific and generic event data becomes more strongly influenced by the plant-specific information as that evidence matures. Incorporation of evidence from additional sites also will allow for the variation of the frequency of events among similar plants (i.e., site-to-site variability). This variability may be the result of unique plant features or because of differences in site characteristics, personnel, and training.

The objective is to derive an estimate of the current frequency for each initiating event. As such, specific cases of data censoring may be both appropriate and desirable. Examples of appropriate data censoring are given below; in all cases, a justification for censoring is mandatory.

9.1.3 Additional Guidance

The original grouping process would have to be revised if the plant records provide different or additional information that indicates the original classification scheme is in error or requires improvement. For example, tripping the main feedwater pumps because of instrumentation indicating a high water level in any steam generator may be listed as a reactor trip due to a high steam generator level. However, these trips are considered more important for the subsequent quantification of a scenario initiated by a loss of feedwater transient than simply a reactor trip, since these trips result in such a condition. Therefore, a strong liaison with the analysts that developed the initiating event grouping is required during this task. Also, it is important to realize that accomplishing the objective of this task requires an engineering perspective that is supported, rather than led, by a statistician.

Many PRAs have assumed that the frequency of initiating events is constant with time. This means the events are statistically random occurrences and the distribution of times between occurrences is exponential. There can be situations when this assumption may not be valid. One such situation is when an implemented plant change (e.g., a modification to plant hardware or procedures) could prevent, or severely curtail, the recurrence of an initiator. Past evidence would then not be representative of the likelihood this event may occur in the future. Therefore, it would be inappropriate to include this evidence in the plant-specific database. It would be inappropriate to include the time period prior to the modification in the database for this initiator as well.

The so-called "learning curve," typically associated with the operation of a new plant, can also influence the rate of occurrence of a particular initiating event. Changes to plant hardware and procedures early in plant life can impact the frequency of initiators. Typically, the first year of commercial operation is excluded from the data in an attempt to reduce the influence of a new plant's "learning curve" on the frequency estimations.

Likewise, the analysts must detect any signs of increasing initiating event frequencies that could be due to the "aging," or wear out, of plant hardware.

Plant trip data must be carefully reviewed to determine if there is evidence of time dependence for specific initiator types. Justification is required for any censoring of data. Censoring may be valid, for example, if, as indicated above, changes to plant hardware or procedures have significantly impacted, or even eliminated, the cause of specific initiators.

Ascher and Feingold (1984) provides guidance for addressing time dependence in reliability analyses.

The term "frequency" is used to describe the measurable, or at least conceptually observable, outcome from experience. Since the outcomes are rarely certain, certainty must be expressed in terms of probability. Thus, the likelihood of a particular class of initiators is expressed in terms of a probabilistic frequency distribution. These distributions can be expressed in several different ways. Kaplan (1981) describes the use of discrete probability distributions. Combining discrete distributions is straightforward, although a scheme of "rebinning" the results is required for practical applications. It is also possible to utilize continuous distributions (e.g., Gamma distributions) to represent the probability of frequency data. The Gamma distribution is one option and is an attractive choice since the update of a Gamma distribution also results in a Gamma distribution. The choice of the distributions form will be determined by the analyst's preference and the calculational tools available.

Generally, initiating events can be assigned to three distinct categories according to the methods applied to determine frequency of occurrence: general transients, transients induced by system failure, and LOCAs (piping failures).

9.1.3.1 General Transients

The general transient category includes reactivity transients and heat removal imbalance transients as well as small LOCAs and very small LOCAs (the latter would include, for example, primary pump seal failures).

The frequency of occurrence of initiators in this category is quantified in a two-step Bayesian process. The first step involves combining the generic evidence (events per year at similar or identical plants) to arrive at a generic initiating event frequency for each initiator group. In the second step, the plant-specific evidence is combined with the generic (population) evidence to arrive at the updated plant-specific initiating event frequency. Details of the formulation of this approach are given in Appendix C.

Regarding the utilization of generic evidence, much has been written and discussed concerning the differences between VVER-1000 plants and VVER-440 plants. There are many differences that can be of significance from a risk assessment point of view. Notwithstanding, it is recommended that the VVER-440 experience not be rejected a priori. It is possible, and indeed likely, that the experience from VVER-440 plants yields relevant data for selected transient initiator categories (such as loss of condenser vacuum and loss-of-offsite power). It is, therefore, recommended that early in the initiating event quantification task each initiator category be carefully reviewed in the context of the relevancy of specific VVER-440 experience.

9.1.3.2 Transients Induced by System Failures

The frequency of occurrence of transients that are the result of a system failure (such as the failure of a support system) are determined using fault trees with the initiating event as the top event (see Section 8.1).

9.1.3.3 Loss-of-Coolant Accidents

The approach taken to quantify LOCA frequencies depends on how LOCAs are classified. If the categories are broadly defined (e.g., large, medium, and small LOCAs), then it may be possible to apply, after careful review, distributions obtained from previous Western analyses. If, on the other hand, LOCAs are more definitively defined (e.g., "LOCA 1" is a failure of the 200-mm pipe between Valve 4-29 and 4-53), then an empirical approach can be adopted, such as the one formulated in Thomas (1981). The Thomas model has been used to express vessel and piping failure rates (for example, see Medhekar, Bley, and Gekler, 1993). A presentation of Thomas' empirical framework, with a modest extension aimed at the application to PRA, is found in Appendix D. It should be noted that the approach would still require data from VVERs or other applicable facilities.

Intersystem (or interfacing) LOCAs involve failure, or inadvertent breach, of a high-pressure/low-pressure boundary. The analysis begins with the systematic identification of all such boundary interfaces. Any available evidence concerning overpressurization (in excess of design values) of piping at VVER plants will be useful. Logic models must be developed

for each LOCA identified, taking into account plant-specific features, such as pressure monitoring and test procedures. Experience in Western PRAs has shown that potential human errors, associated with the testing of valves that are part of the high-pressure/low-pressure boundary, are important in estimating occurrence frequency.

9.1.4 Deliverables

As identified in the task Documentation (Chapter 3), the current task will produce draft material for the final report. Specifically, a draft of a portion of the "Initiating Event Analysis and Quantification" appendix to the PRA Main Report and a draft of the "Initiating Event Frequency" portion of the Backup Documentation constitute deliverables for this task. In addition, this task is responsible for producing the frequency information in electronic form suitable for use in the sequence quantification activity.

9.2 Component Reliability

The objective of this task is to obtain plant-specific estimates of the unavailability of specific equipment used for PRA quantification. The scope of this task is to develop the database needed for estimating the contributors to unavailability of the basic events modeled in system fault trees. The task also includes developing component failure models, collecting generic and plant-specific component data, and estimating the parameters of the component unavailability models. It is important that the component unavailabilities are expressed in the form of uncertainty distributions and that similar components be grouped in the same correlation class. Assigning a group of components to a correlation class implies that a fully dependent Monte Carlo sampling routine would be utilized for the uncertainty evaluation. Therefore, the uncertainty distributions for all components in a correlation class should be the same. The experience data for all similar components belonging to a correlation class could be used for the estimation of the uncertainty distribution. Typically, components of the same type exposed to approximately the same environment, and with similar normal operating conditions, are grouped in the same correlation class (e.g., all normally energized DC relays).

9.2.1 Relation to Other Tasks

The activities for this task can be understood by reference (refer to Figure 9.1) to the tasks with which it interfaces:

Plant Familiarization (Chapter 2). The identification of plant-specific data sources for estimating component failure parameters is initiated as a part of this task. In the current task, the plant-specific data are collected and used in combination with generic data to estimate the component failure parameters.

System Modeling (Section 8.1). The output of the current task provides input to the task System Modeling. During the preliminary development of system models, generic component data is usually adequate. The component failure parameters estimated using plant-specific data have to be provided before the system fault trees can be finalized. The level at which data analyses are to be performed (component, train, etc.) for various unavailability contributors, the boundary of the equipment, and the associated failure modes should be coordinated between these two tasks (System Modeling and Component Reliability).

Frequency of Initiating Events (Section 9.1 above and Chapter 6). Estimation techniques used for component failure unavailability contributors are similar to those for initiating event frequencies. Consistency in the methods and software used should be maintained. The impact of initiating events on the unavailability of some basic events may be determined using data analysis–for example, the probability of loss-of-offsite power after a generator trip.

Common-Cause Failure Probabilities (Section 9.3 below). The method and software used in estimating initiating event frequency and estimating common-cause failure probabilities should be consistent. The plant-specific database developed in the current task could be used for estimating the plant-specific common-cause failure probability estimation.

Initial Quantification of Accident Sequences (Chapter 11). Component failure parameters, by providing input to system modeling, are indirect

input needed for quantification of accident sequences.

9.2.2 Task Activities

The unavailability of a component can be thought of as the fraction of time that a component could not meet its demand successfully, either because it is unavailable due to test or maintenance or it resides in a failed state. Generally speaking, the unavailability is the probability that a component does not perform its intended function when required, and, therefore, it can also encompass the failure probability per demand. This procedure guide focuses on estimating the following parameters of equipment unavailabilities:

- Component failure rates expressed in terms of "failure per unit time" or "failure on demand,"
- Frequency and duration of corrective (unscheduled) maintenance,
- Frequency and duration of preventive (scheduled) maintenance, and
- Frequency and duration of testing.

The estimations of the above parameters are necessary to evaluate the direct contributors to unavailability from hardware failure, maintenance, and testing. Other contributors to unavailability resulting from inadvertently leaving a train in an unavailable state after a test or maintenance should be identified and evaluated jointly with the system fault tree (see Section 8.1) and human reliability analysis (see Chapter 10). The general process for this task is:

1. Determine the most appropriate level, scope, hardware boundary, and specifications for data collection through coordination with the teams that performed system fault trees and event trees,

2. Establish the current knowledge on the parameters to be estimated by aggregating the various sources of generic data and the experience of similar plants,

3. Identify the sources of plant-specific data to be retrieved, reduced, reviewed, and interpreted for the parameters of interest and establish the plant-specific data summary, and

4. Combine plant-specific and generic data when appropriate to estimate the needed parameters and to reflect the associated uncertainties.

There are several assumptions and simplifications that are currently used in state-of-the-art PRAs. Awareness of these assumptions and their verification to the extent possible is an important task in performing PRAs.

- Component failure rates are assumed to be constant and time invariant. This is a limiting assumption that stems from the simplifications that are typically made in PRA quantification routines. This assumption does not allow the modeling of any aging or wear out mechanism, and, therefore, it does not allow proper modeling of the benefits of maintenance and in-service testing in terms of preventing the aging mechanisms.

- Interpretation of what constitutes a failure depends on the mission and function of the equipment. Engineering review of the failure events are necessary to decide whether a reported event is indicative of a component's failure occurrence with a predefined boundary.

- Operational testing of a component is typically treated as an ideal test capable of detecting every type of failure and failure mode. Since most of the tests performed on the components do not simulate actual demand conditions, the tests will not be able to detect all possible failures and failure modes. The PRA analyst should review the test procedure and decide whether a test should be credited for all possible failure modes. Motor-operated valve (MOV) testing practice in the U.S. is an example of an incomplete test. The MOVs are typically tested with a smaller pressure drop across them than is typically experienced in actual demands. The test, therefore, cannot verify if the MOVs will close against the full accident pressure

differential. In this case, special testing for selected MOVs based on their risk significance are implemented to assure their proper operation. Other examples of incomplete testing are the tests that use the mini-flow path of a pump train. Here, the test only verifies the proper closure of the breaker's contacts and the operation of the valve stem for the pump discharge valve under a no-flow (static) condition.

- Test-caused failures and human errors resulting in a component or train being left in an unavailable state after the test are incorporated in the system fault tree model through coordination with the human reliability analysis. Sometimes the human error rates for such events can be estimated directly as part of a data analysis task and incorporated as part of component unavailability. Care should be taken to assure that such events are properly identified, the human reliability analyst is consulted, and the fault exposure time for such failure mechanisms is set to a full test interval (rather than one-half test interval).

- Uncertainty distributions of the expected unavailability of a component are typically assumed to be lognormally distributed. This assumption, though widely practiced, is not necessary. The uncertainty distribution for component unavailability largely stems from the uncertainties associated with the failure rate of the component. The uncertainties associated with the other parameters in the component reliability models, e.g., the average repair time, are sometimes not accounted for. This is because of difficulties generally encountered using current computer codes. For example, the Integrated Reliability and Risk Analysis System (IRRAS) code does not allow the analyst to define uncertainties for both the frequency and duration of unscheduled maintenances. To account for both types of uncertainties, the analyst should estimate the resulting unavailability contribution and the associated uncertainty outside the IRRAS code and then input the results to IRRAS.

- The failure rate of a component in the harsh environment of an accident is usually estimated based on the deterministic criteria derived from test results, engineering evaluation, and subjective judgments. Examples are equipment survivability in a boiling water reactor building after drywell failure, the equipment survivability in a steam-filled room, or failure of the electrical and electronic equipment in the switchgear room after loss of the heating, ventilation, and air conditioning system.

- The failure rate associated with rupture of the component boundary and pipe rupture is typically estimated based on generic data, performing simple fracture mechanic calculations, and using semi-empirical models or subjective judgment.

The above assumptions and limitations are inherent in the reliability assessment of components for PRA use. The uncertainties associated with the component reliability should reflect the analyst's current level of knowledge for the failure mode of concern. The analyst may initially perform the PRA calculations using crude conservative estimates, followed by more rigorous analyses commensurate with the risk importance of the components.

9.2.3 Additional Guidance

Assessment of the component reliability involves modeling and estimation of all the contributors to component unavailability. For this purpose, the components are typically categorized in two groups: standby and operating components. The unavailability models of interest for each group are described below, and the specific parameters to be estimated in the data analysis task are identified.

9.2.3.1 Standby Component

A standby component is a piece of hardware with a predefined boundary that is normally in a state different from the state of its safety function. As an example, a normally open valve (normal state) is expected to close (state of its safety function) in certain scenarios. This valve is considered a standby component since its normal and safety

states are different. A standby component can have many failure modes, some of which can be detected when the component is in its normal state and others when the component is periodically tested for its safety function. In the earlier example, failure modes, such as the housing rupture or leakage, could be detected when the valve is in its normal state, whereas the valve actuator failure preventing the valve closure can only be detected during the periodic tests. The expected time to detection of a failure is referred to as fault exposure time. For those failure modes detectable by periodic testing, the fault exposure time is one-half the periodic test interval. If certain failure modes can be detected by other activities, such as a walk through or visual inspection, the fault exposure time would be one-half the inspection interval. Finally, some failure modes can be detected almost instantaneously--for example, by alarm or valve position indicator. In this case, the fault exposure time associated with the failure mode is zero, and the standby component for that failure mode is referred to as a monitored component.

Various contributors to standby component unavailability are:

- fault exposure time, i.e., failure during standby
- failure to start or failure on demand
- failure during mission time
- testing
- unscheduled corrective repair
- scheduled preventive repair.

Table 9-1 provides a summary of the formulas to be used to estimate each contributor and identifies the specific parameters to be estimated by reliability data analysis. The last column in the table shows the needed summary event data for the specific plant under study. Deterministic data from sources, such as plant technical specifications, is not listed in this column. The total component unavailability would be the sum of all its contributors.

9.2.3.2 Operating Component

An operating component is a piece of hardware with a predefined boundary that is normally in an operating state consistent with its safety function. Failure of an operating component could contribute to an initiator frequency (see Section 9.1). Failure of an operating component after the occurrence of the initiator is typically modeled within the system fault trees and is the focus of the discussion here. The two major contributors to the unavailability of an operating component are:

1. Unavailability due to repair: An operating component may be unavailable as a result of failure prior to an initiator and may remain unavailable after the occurrence of the initiator. This unavailability could be simply estimated using the following equation:

$$Q_R = (\lambda_R T_R)/(1+\lambda_R T_R)$$

where λ_R, and T_R are defined in Table 9-1. Note that all causes for performing corrective and preventive maintenances are incuded in estimating the rate λ_R.

2. Unavailability due to failure during the mission time after the occurrence of the initiator. This unavailability could be simply estimated using the following equation:

$$Q_M = (\lambda T_M)$$

Here, λ is the actual failure rate of the operating component and does not include any degraded conditions, and T_M is the expected mission time associated with the component.

All contributors to component unavailability for both standby and operating components could be subjected to recovery action if sufficient time is available for returning the component to an operational state. As an example, there could be up to several hours available before a room containing safety equipment heats up to a critical temperature after loss of a cooling fan. The probability of successful recovery actions either by repairing the affected components or by providing an alternate means for performing the needed function should be typically modeled at an accident sequence or accident minimal cutset level after the event trees without recovery are quantified.

9.2.3.3 Plant-Specific Data Collection, Interpretation, and Evaluation

Past experience with PRA data collection activities has shown that no single data source in the plant is sufficient to provide all the needed information. PRA practitioners had to search through various sources of data to properly identify and interpret a single record. Plant design documentation, operator logs, maintenance records, plant technical specifications, and surveillance procedures constitute the minimum set of information typically examined for determining the data needs for use in a PRA. Event data of interest for component reliability evaluation are (1) information relating to component performance in response to a test or an actual demand and (2) information relating to component down time during testing and maintenance. Information on component performance in response to a test or a demand should be interpreted or categorized as failure, degraded, or success. Failure encompasses all events that render the component either outside the acceptable envelope of the technical specifications or within the PRA definition of the failure and the failure modes of the component under study. Degradation encompasses those events that indicate that the component is not in a failed state; however, it could fail eventually if it is not repaired. Generally, all unscheduled repairs triggered by unsatisfactory performance of the component but not by its failure are categorized as degradations. Some PRA data evaluations have broken down the degradations into degraded and incipient conditions depending on the severity of the fault and the available time before the condition propagates to a failure. Another area of data analysis that may require extensive interpretation deals with component recovery probability. A component may be made available during certain testing procedures if an actual demand occurs. A failed component could also be made available for certain failure modes. Such recovery actions typically require manual actions (e.g., realignment of a suction path or manual start of a pump). These probabilities for recovery actions should always be reviewed by human reliability analysts, even if in some cases the probabilities could be estimated based on the experience data. Generally, interpretation of collected data is a multi-disciplinary task that requires close cooperation between PRA data analysts, PRA system analysts, PRA human factor specialists, and plant operation and maintenance staff.

9.2.3.4 Methods for Estimation

Various parameters derived from the component reliability models are identified for both standby and operating components. Some of these parameters, such as periodic test interval and the preventive maintenance frequency, could be obtained directly from plant-specific procedures and technical specifications. These types of parameters typically are not statistical in nature and are treated as deterministic information. The remainder of the parameters, such as corrective maintenance rate, are statistical in nature and should be estimated based on plant-specific and generic data sources. Currently, Bayesian analysis is widely accepted as the estimation method. The single-stage Bayesian approach is commonly used for estimating the parameters for component reliability models when the generic reliability database provides the estimates of the parameters of the prior distribution. The two-stage Bayesian approach could be utilized when the generic database contains summary data for other plants (e.g., number of failures and the observation period). The theoretical basis for the Bayesian approach and formulation and some available software has been extensively discussed in the open literature, e.g., Apostolakis et al., 1980 and Apostolakis, 1982. The following provides a discussion on the single-stage Bayesian approach. For the two-stage Bayesian routine, the task on initiating event frequency may be consulted.

9.2.3.5 Prior Distribution

The Bayesian approach requires the use of a prior distribution for the parameters to be estimated. Prior distributions are typically obtained from industry-wide data analyses. In some cases, a prior distribution is generated from the failure rate estimates reported in past PRAs. In this situation, the analyst should combine the data from several PRA sources to arrive at one single prior distribution representing plant-to-plant variability. There are several different ways suggested in the past for combining multiple distributions to develop a generic prior distribution

Table 9-1 The reliability formulation for the various contributors to the unavailability of a standby component

Unavailability Contributor	Reliability Formula	Model Parameters	Summary Data Needed
Fault exposure time	$1-(1-e^{-\lambda T})/(\lambda T)$ or $\approx (½)\lambda T$	λ: Standby failure rate T: Surveillance interval	Number of failures and the total observation period
Failure to start or failure on demand	Q_d	Q_d : Failure to start per demand or failure on demand	Number of start or demand failures and the total number of demands
Failure to complete the mission	$\lambda_R\ \theta$	λ_R: Running failure rate θ: Mission time	Number of failures and total operating time
Periodic testing	$(\tau/T_p)\ P_r$	τ: Expected test duration T_p: Periodic test interval P_r: Failure probability to override or recover from the test	Number of times the test override was needed and the number of times it failed
Unscheduled corrective repair	$(\lambda+\lambda_D)T_R$	λ_D: The rate of degraded conditions that require corrective maintenance T_R: Mean repair time	Number of degraded conditions and total observation time Duration of corrective maintenance
Scheduled preventive repair	$f_m\ T_m$	f_m: Frequency of preventive maintenance T_m: Expected duration of preventive maintenance	Duration of preventive maintenance averaged over all different types

Notes:

- For monitored failure modes T = 0.
- For those failure modes detectable by other surveillance activities (e.g., visual inspection) in addition to periodic testing, T can be estimated by the total time period divided by the number of surveillance activities (periodic or otherwise).
- For those failure modes not detectable by any surveillance activities, T should be set equal to the remaining plant lifetime since the last time component was verified operable (e.g., for a new plant with an expected service life of 40 years, T = 40 years) and approximate formulae should not be used.
- For all other cases $T = T_p$.
- All failure rates should be expressed in terms of time-related failure rates to the extent possible to assure consistency. For some components, such as the emergency diesel generators, component failures are divided into standby failure, start failure, and run failure. For other components, such as failure of a motor operated valve to open/close, the generic data is reported as failure probability on demand. Probability of demand failure could be translated into the equivalent time-related failure rate, if so desired, by dividing the demand failure probability by one-half of the expected time between the demands (typically the periodic test interval).
- For those human errors modeled in fault trees which indicate leaving a train in an inoperable state after test or maintenance, the fault exposure time to be used is the full surveillance interval. The unavailability contributions for such human errors should be kept separately, and a separate test caused unavailability should be estimated.
- λ_D is estimated similar to the failure rate λ. λ_D is the rate of unscheduled maintenance. It is estimated based on the number of times, within the data collection period, that a component underwent repair (corrective unscheduled maintenance) even though it was not yet failed.
- $(1-P_r)$ is the probability of making a component or train available during a surveillance test if an actual demand occurs. In most practical cases, the value of P_r is either zero or one, respectively, indicating that the unavailability due to a test is either easily recoverable or unrecoverable in time. In those special cases where the available recovery time and the time needed to recover from the test are comparable, the value P_r should be determined with help from the human reliability analyst.

(Gentillon, 1987; Martz and Bryson, 1984; and Azarm and Chu, 1991). A method typically used to arrive at a generic prior distribution is by constructing a mixture distribution from all sources. The weights associated with different sources are typically the same as long as all the sources are applicable to the type, boundary, and the failure mode of the component under study. In some cases, different weights are assigned depending on the extent to which the generic sources represent the basic event under study. A different method to assure that the resulting generic distribution has a wide enough uncertainty to reflect faithfully differences among all the sources is reported (Azarm and Chu, 1991). The choice of method to use is up to the analyst; however, the analyst should examine the constructed generic distribution to see if it does cover all the means reported by various sources within its 5th and 95th percentiles .

9.2.3.6 Likelihood

The Poisson and Binomial likelihoods for failure rate per hour and failure rate per demand are discussed for the task Frequency of initiating Events. However, these likelihood functions are not appropriate for Bayesian updating of the distribution for the repair duration. Here, the likelihood may simply be a non-reducible, joint-probability distribution for repair durations observed, sometimes referred to as sampling likelihood. Since this likelihood is not incorporated in the widely used Bayesian codes, the analyst may decide not to use the Bayesian approach in determining the mean repair distribution especially since the uncertainties associated with mean repair time are not commonly accounted for in the PRA. In summary, the likelihood function should, to the extent possible, reflect the process through which the data was generated and collected.

9.2.3.7 Posterior Distribution

The commonly used Bayesian software automatically generates a posterior distribution and typically outputs the associated parameters of a fitted lognormal distribution. An examination of the posterior distribution by the analyst should be done to assure its appropriateness. This is typically done in three steps. In the first step, the posterior distribution is compared with the prior distribution. If the mean and variance of the prior are distinctly different from that of the posterior distribution (a factor of 2 or more), then the analyst should verify that the data shows strong evidence. For data to strongly affect both the mean and the uncertainty of the posterior distribution (i.e., considered to be strong evidence), the data should contain at least three independent observations. In the second step, the analyst should check the evidence data to make sure that the data is not strongly affected by the failures of one component in the group. In some cases, a component failure may not have been diagnosed properly and the repair was incomplete, thereby making the same component fail several times within a short period of time. Such clustered data should be detected and resolved. In the third step, the analyst should assure the adequacy of a lognormal fit to the posterior distribution. The reader should note that the use of a lognormal distribution is not essential when using the IRRAS code even though it has been widely practiced in the past. Some posterior distributions may not resemble a lognormal distribution; therefore, the fitted lognormal distribution based on matching the first two moments may not be appropriate. In such cases, a more appropriate fit may be obtained by conserving the mean and the 95th percentile of the distribution rather than the mean and variance. Also, special care should be given to those cases when trying to use the Bayesian approach with zero failure as the evidence. Updating of the generic failure rate with the evidence of zero failure is not typically recommended unless the observation period is at least twice the expected mean time to failure derived from generic prior.

9.2.4 Deliverables

This task has two deliverables. First, a generic component database based on generic VVER data should be developed and supplied to the system analysis task in support of fault tree development. The generic data can also be used in the initial quantification of the event tree sequences. For final quantification of the accident sequences, a plant-specific database has to be used.

The documentation of this task should include descriptions of the sources of generic and

plant-specific data, descriptions of the component failure models used, a summary of plant-specific failure events, a description of the statistical methods and software used in estimating failure parameters, and tables of both generic and plant-specific data that can be used to calculate the basic event probabilities used in the PRA. Any assumptions made in the analysis, e.g., in interpreting plant-specific data and their application to estimating failure parameters, should be clearly documented. The component database should cover all the parameters shown in Table 9-1.

9.3 Common-Cause Failure Probabilities

The objective of this task is to determine the final values to be used in the parametric models of common-cause failures (CCFs). This would involve addressing a variety of issues starting with defining what should be considered as CCFs, how they should be modeled in the context of system fault trees, and finally how they are to be estimated using generic and plant-specific (Kalinin-specific) data. Specific areas that will be addressed in this procedure guide are:

- sources of generic data,
- component types for CCFs,
- failure modes for CCFs,
- cause considerations for CCFs,
- component grouping rule for CCFs within a system,
- component grouping rule for CCFs across systems,
- CCF considerations for plant-specific data collection, and
- estimation of the CCF contributors.

9.3.1 Relation to Other Tasks

As discussed earlier, there is an explicit relationship between CCF modeling and the scope/level of detail in the PRA (Chapter 5). There is also direct interaction between this task and the task System Modeling (Section 8.1) in the area of grouping and modeling of the CCF components. The analysis of plant-specific data as a potential source for obtaining estimates of CCF and the use of CCF generic data also establish a strong link between this task and the task Component Reliability (Section 9.2 above). The estimated CCF parameters are then used in the initial and final quantifications and sensitivity evaluations (Chapter 11). The types of interactions expected from this task to other interrelated tasks are not simply in the form of input/output, rather it involves two-way interactions. As an example, the initial quantification task uses the generic CCF parameters as input; however, this task will identify important CCF groups for which more detailed CCF analysis and estimation would be needed. Similarly, this task would describe specific guidelines for component grouping for modeling of CCF events which will be used in the system fault trees (Section 8.1) and for which this task would estimate CCF parameters.

9.3.2 Task Activities

There are generally two major limitations associated with the modeling of CCFs in a PRA. One limitation deals with whether the identification of CCFs is adequate to assure that the modeled CCFs are comprehensive but not duplicative, and the other limitation deals with the applicability of the CCF generic data to the specific plant being studied.

The definition of CCFs is interrelated with the scope and the level of detail in the PRA. For example, in the early eighties when PRAs were of limited scope, an event would have been categorized as CCF if more than one failure due to any of the following causes was observed:

1. fire, flood, seismic, or any other external event,
2. high temperature, such as loss of heating, ventilation, and air conditioning system,
3. pre- and post-initiator human errors disabling multiple components,.
4. design and installation problems, e.g., wrong materials,
5. procedural problems,
6. aging and wear out,
7. temporary degradation of components due to such causes as improper maintenance and surveillance, and
8. sneak circuits and unexpected interdependencies.

However, as the scope, modeling complexities, and the level of detail in PRAs increased, characterization of CCF matured allowing them to be modeled more explicitly. For example, the analysis performed to evaluate external event PRAs, the formal modeling used to directly address loss of the heating, ventilation, and air conditioning system (either as an initiator or as a part of a system fault tree), and the explicit modeling employed to quantify pre- and post-initiator human error rates eliminated the need to distinguish Categories 1, 2, and 3. Furthermore, the probability of CCF can be reduced significantly once certain CCF failure mechanisms are observed and subsequent corrective actions are taken, as, for example, in Categories 4 and 5. When design/installation problems and/or procedural deficiencies are detected, corrective actions are usually put in place to rectify the problems to the extent possible. Finally, some of the sneak circuits and unexpected interdependencies could be identified while in the process of conducting a relatively detailed PRA. Consequently, CCF estimates have changed over time as PRAs increased in scope and level of detail. Therefore, CCF estimates are only used to capture those events that are not explicitly modeled in PRAs. The more the scope and level of detail in a PRA, the less would be the number of dependent events not explicitly accounted for in the PRA. Also, some have argued that the CCF estimates should also capture and compensate for the inadequacies inherent in simplified PRA quantification algorithms (see Azarm et al., 1993). PRAs performed in the U.S. typically use generic data on CCFs, at least initially. However, even for this initial use, the generic data must be tailored for the specific plant. This is typically done by mapping the industry-wide events (data) against the scope of the PRA, its level of detail, and the current plant practices in order to identify and use the subset of the events that are most applicable to the plant. Recently, a published six-volume report by the U.S. Nuclear Regulatory Commission on CCF (Stromberg, 1995) provides a computerized database of the latest U.S. study on generic CCF estimates.

It is recommended that CCF modeling be performed in two phases. For the first phase, CCF probabilities are to be estimated based on the applicable industry-wide CCF events. The plant models then should be quantified, and the major CCF contributors identified. For those CCF events which significantly contribute to plant risk, further analysis is needed to justify that the CCF estimates are appropriate. The results of these analyses should be explicitly discussed with plant staff and regulators for identification of potential corrective actions. This would constitute the second phase analysis. The final estimates including the impact of any potential corrective actions on the CCF rates should be used for final quantification.

9.3.2.1 Activity 1 — Generic Data

The sources of generic data are identified and the associated CCF events are reviewed to verify applicability to the specific plant, i.e., establishing generic data which is tailored for the Kalinin Nuclear Power Station (KNPS).

9.3.2.2 Activity 2 — CCF Rules

The CCF rules for component types and component grouping within and across systems are communicated to system modelers to assure consistency in modeling.

9.3.2.3 Activity 3 — Plant-Specific Data

Plant-specific data indicative of potential CCF occurrences are collected. A potential CCF involves occurrence of multiple failures that are suspected to have been caused by CCF triggering mechanisms. The corrective actions which could possibly eliminate the triggering mechanisms are not given credit at this stage. A Bayesian routine is used for updating the CCF parameters.

9.3.2.4 Activity 4 — Initial Quantification

Initial quantification and the associated sensitivity and importance evaluations are performed to identify those CCF events that are risk significant.

9.3.2.5 Activity 5 — Final Quantification

Detailed analysis, either qualitative or quantitative, whichever is more appropriate, is conducted to adjust the baseline estimates of the risk significant CCFs.

9.3.3 Additional Guidance

9.3.3.1 Sources of Generic Data

The database for the CCF events developed in the U.S. (reported in Stromberg, 1995) should be used as one of the data sources. The event data should be reviewed and those events that are either duplicative (due to scope and level of effort in the KNPS PRA) or are not applicable (due to specific features of KNPS) should be discarded. New CCF rates should be estimated with the remainder of the CCF events. However, in some generic sources of data, the event description may not be available or summarized so that its applicability to a specific plant may not be verifiable. In these cases, a certain degree of subjectivity or conservatism may be applied. Additional data for CCF not currently included in the Idaho National Engineering Laboratory report (Stromberg, 1995), e.g., data on instrumentation and control components, relays, transducers, is provided in Appendix E.

9.3.3.2 Component Types for CCFs

Volume 6 of the Idaho National Engineering Laboratory report specifically identifies various components for which CCF estimates were determined. However, the component types are categorized based on systems in U.S. pressurized water reactors and boiling water reactors, e.g., pumps in the Service Water System. Generic component types, such as MOVs, without any further categorizations based on systems or any other feature could be sufficient for most CCF modeling applications. Further classifications of MOVs (for example, to differentiate low-pressure or high-pressure applications) should only be performed if supported by data. Appropriate data searches and CCF estimations should be performed using the database structure in the reference cited to assess whether the CCF estimates significantly change if MOVs are further categorized by low-pressure or high-pressure application. It is also recommended that the number of component types should be kept as small as possible to make the estimates manageable. The breakdown of a component type based on environment, size, and stress (e.g., pressure) should not be done unless justified by the data. Several different CCF estimates could be obtained generically for a component type for different failure modes, initial conditions, and given service applications. These considerations are some of the bases for the CCF grouping that are discussed under Component Grouping Rule for CCFs Within a System and Component Grouping Rule for CCFs Across Systems.

9.3.3.3 Failure Modes for CCFs

Various component failure modes should be differentiated in CCF modeling when different failure modes result in different consequences. For example, two different failure modes, failure to open and failure to control (stuck in an intermediate position), may be considered for a standby control valve. If these two different failure modes result in different consequences (in terms of system or plant responses), the failures should be kept separate and the CCF data should be differentiated.

9.3.3.4 Cause Considerations for CCFs

To develop a complete understanding of the potential for multiple failures, it is necessary to identify the reasons why these types of failures occurred. Understanding the causes of the CCFs is important in evaluating both the event data and proposed plant defenses against CCF occurrences. Cause classifications proposed in Volume 2 of the Idaho National Engineering Laboratory report could generally be used. Furthermore, the examples provided in this volume are constructive in assuring consistent understanding of cause classification for CCFs.

9.3.3.5 Component Grouping Rule for CCFs Within a System

A set of components within a system that could be represented by a common-cause group are discussed using the following simple one-line diagram (Figure 9.2):

All six valves in suction and discharge may be considered as a CCF group. In this case, specific combinations of multiple (three or more) failures are considered to result in system failure. However, the discharge valves are located inside containment, and they are neither tested similar to nor as frequently as the suction valves. Hence, the analyst should consider two CCF groups: one for valves V1A, V2A, and V3A and the other for

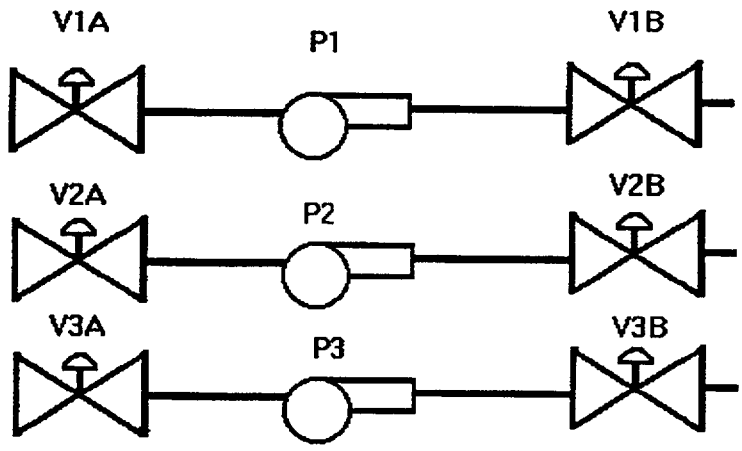


Figure 9.2 Simple example for CCF analysis

valves V1B, V2B, and V3B. The contribution of the CCF, and consequently the system unavailability, would be different in these two cases. The latter would typically result in a lower system unavailability estimate for the same combinations of basic events. Therefore, rules should be provided to assure proper grouping of CCF components, thereby preventing potential underestimation of system unavailabilities.Since there are no step-by-step rules that can be written for prescribing how to group components for CCF, only general guidance can be provided to assist the analysts. A minimum set of considerations that could be used by the analysts for component grouping for CCFs are:

- types of components with some regard as to their application, size, function, etc.,
- the normal operational state and the failure mode of the component,
- the operational activities, such as tests and maintenances, and their associated frequencies, and
- similar location and exposure environment.

It is also recommended that like components produced by different manufacturers do not necessarily imply that the components belong to separate CCF groups. Similar components from CCF groups only if the following two conditions are met:

1. The components do not belong to a natural or to a logical redundancy, as do valves V1A, V2A, and V3A in the above example. There is no justification to have separate groupings for these valves if one of the valves was manufactured by Company XYZ, for example, and the other two were not. However, if the discharge valves V1B, V2B, and V3B are from Company XYZ and the suction valves are not, then there might be some justification for different groups, if the next condition is met.

2. The industry data should indicate that manufacturing and design specifications were the major contributors to the CCF estimates. In this case, separate grouping could be used if additional engineering justifications can be provided to show that the components from different manufacturers exhibit different CCF characteristics.

Dividing the CCF grouping based on the manufacturer should be a last resort and should be avoided to the extent possible.

9.3.3.6 Component Grouping Rule for CCFs Across Systems

Across-system CCFs are not typically modeled in U.S. PRAs. However, the analysts should be

aware that although this type of CCF grouping is possible, it should not be formed by artificial logical boundaries made as a result of fault tree modeling. Rather, it is recommended that the final accident sequence minimal cutsets be reviewed, and based on the criteria provided in Component Grouping Rule for CCFs Within A System, the analyst should identify those component groups across systems for which CCF modeling need be considered. Since an across-system CCF group may involve a large number of components, the CCF parametric modeling can become unmanageable. The number of combinations to be used in CCF parametric modeling should be limited. For example, if the multiple greek letter model is used, factors for five components will be applied to all components in the group (if five fails all fails).

9.3.3.7 CCF Considerations for Plant-Specific Data Collection

The system analyst should provide to the data analyst the list of components in the CCF groups for data collection and interpretation. Whenever a component from a CCF group has failed, a data field in the data sheet (to be filled in by data analyst) should indicate a request for information on simultaneous failures of similar components or recent failures that have occurred over a short period of time. The following definitions for simultaneous and recent failures are suggested:

1. For sequentially tested, standby components, simultaneous failures are defined as failures that have occurred within a time period less than one test interval. For standby components that are tested in a staggered fashion, simultaneous failures are those that have occurred in less than one-half the test interval. For operating components failures that have occurred within the PRA mission time are considered as simultaneous failures.

2. Recent failures are defined as failures that have occurred in a time period that is less than one failure time. To calculate the failure time, the generic mean time between the failures of the component should be divided by the number of the components in the group. As an example, if there are five components in the group and the generic failure rate for the component is 1.0×10^{-4} per hour (or the mean time between failures is 1.0×10^{4} hours), the recent period would be 2000 hours (or approximately about three months). If similar failures on this component group have occurred over a three-month time period or less, these failure histories should be queried for possible common-cause connotations.

The system analyst and the data analyst should work closely together to ensure that the data queries will capture the requisite information needed for parametric estimation of CCFs.

9.3.3.8 Estimation of the CCF Contributors

Currently, there are four types of methods that could be utilized for estimating the CCF rates. Two of these methods are typically used in early stages of the analysis (Phase 1), whereas the other two methods are typically done after initial quantification (Phase 2). In Phase 1, the actual CCF events from a generic database are reviewed and evaluated against the specific features of the plant design, the current plant practices, and the PRA. This allows the user to specialize events for application to a specific plant by assigning an applicability factor to each event. The applicability factor is a value between zero and one. The higher the applicability factor, the more relevant the event would be to the specific plant being studied. There are some degrees of subjectivity involved in assigning an applicability factor. To use the estimation methodology of Stromberg (1995), an event-by-event assessment is required to determine the values for three classes of applicability factors. These are R1, Cause Applicability Factor; R2, Coupling Applicability Factor; and R3, Failure Model Applicability Factor. There are some discussions on the assignment of these applicability factors in Mosleh et al. (1989).

The second type of analysis that could be performed deals with the use of plant-specific CCF events. Updating of generic estimates with plant-specific CCF data would be performed for those cases where multiple simultaneous failures have occurred and are suspected to have been caused by CCF mechanisms. The Bayesian update of the CCF model parameters is generally not a straightforward procedure (except for some

specific CCF models, such as the global Beta factor model) and could involve extensive computations. There are two alternative approaches that could be pursued for plant-specific updating of generic data. One approach is to treat plant-specific data as a part of specialized generic data and to select the value of one for the applicability factor. The impact of the plant-specific data in this approach would depend on the size and quality of generic data (e.g., number of CCFs and number of demands in the generic database). The higher the quality of the specialized generic data, the less would be the impact of plant-specific data. The other alternative could be to estimate the CCF model parameters based on plant-specific data when possible and to use the weighted average of plant-specific and generic data. The weighting factor would be subjective depending on the analyst's confidence in generic vs. plant-specific data. The final aggregate results for the CCF parameters should conserve the constraints imposed by the specific CCF model used.

In the Phase 2 evaluation, the CCF estimates could be adjusted based on qualitative reasoning on the current plant practices in the areas of defenses against CCFs including the corrective actions proposed by the plant. Methods reported by Bourne et al. (1981) and by Humpherys (1987a, 1987b) are candidates for this type of analysis. Quantitative analyses could also be performed in the Phase 2 evaluation based on failure time statistics. In this regard, plant-specific data on times of component failures in the CCF group should be collected including any simultaneous failures. Since it is not expected that much data on multiple simultaneous failures is to be found for use in the Kalinin PRA, reliance on predicting CCF probabilities based on statistical correlation of failure times (clustering) would be the only option. A method for performing such analysis based on clustering of failure times is described in Azarm et al. (1993).

9.3.4 Deliverables

1. A KNPS-specific document providing information on the scope of CCF to be modeled including component types and grouping. It should also identify the CCF parametric models to be used including the ways that it could be incorporated in system fault trees. The document should be distributed among all system and data analysts.

2. A KNPS-specific CCF rate including a description of approaches used in arriving at those estimates should be documented. These estimates would be utilized in the first phase analysis.

3. The risk significant CCFs identified through initial quantifications and the results of sensitivity and importance evaluation should be documented and used for the refined CCF estimates for the second phase analysis and final quantification.

4. The final set of CCF rates generated through the second phase analysis should be documented for use in the final quantification.

9.4 References

Apostolakis, G., "Data Analysis in Risk Assessments," *Nuclear Engineering and Design, 71*, pp. 375-381, 1982.

Apostolakis, G., et al., "Data Specialization for Plant-Specific Risk Studies," *Nuclear Engineering and Design, 56*, pp. 321-329, 1980.

Ascher, H., and H. Feingold, Repairable Systems Reliability, Marcel Dekker, Inc., New York, 1984.

Azarm, M. A., et al., "Methods for Dependency Estimation and System Unavailability Evaluation Based on Failure Data Statistics," NUREG/CR-5993, Vols. 1 and 2, Brookhaven National Laboratory, July 1993.

Azarm, M. A., and T.-L. Chu, "On Combining the Generic Failure Data for Probabilistic Risk Assessment," Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM), February 4-7, 1991.

Bourne, A. J., et al., "Defences Against Common-Mode Failures in Redundancy Systems," SRD-R196, Safety Reliability Directorate, January 1981.

Gentillon, C. D., "Aggregation Methods for Component Failure Data in the Nuclear

Computerized Library for Assessing Reactor Reliability," EGG-REQ-7775, Idaho National Engineering Laboratory, 1987.

Humpherys, P., et al., "Design Defences Against Multiple Related Failures," Advanced Seminar on Common-Cause Failure Analysis in Probabilistic Safety Assessment, Kluwer Academic Publication, edited by A. Amendola, pp. 47-57, ISPRA, Italy, November 16-19, 1987a.

Humpherys, P., et al., "Analysis Procedures for Identification of Multiple Related Failures," Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, Kluwer Academic Publication, edited by A. Amendola, pp. 113-129, ISPRA, Italy, November 16-19, 1987b.

Kaplan, S., "On the Method of Discrete Probability Distributions in Risk and Reliability Calculations--Application to Seismic Risk Assessment," *Risk Analysis*, 1, pp. 189-196, 1981.

Martz, H. F., and M. C. Bryson, "A Statistical Model for Combining Biases in Expert Opinions," IEEE Transaction on Reliability R-33, August 1984.

Medhekar, S. R., D. C. Bley, and W. C. Gekler, "Prediction of Vessel and Piping Failure Rates in Chemical Process Plants Using the Thomas Model," Process Safety Progress, Vol. 12, pp. 123-126, April 1993.

Mosleh, A., et al., "Procedure for Treating Common-Cause Failure in Safety and Reliability Studies: Analytical Background and Techniques," NUREG/CR-4780, Vol. 2, U.S. Nuclear Regulatory Commission, January 1989.

Stromberg, H. M., et al., "Common-Cause Failure Data Collection and Analysis System", Vols. 1 through 6, INEL-94/0064, Idaho National Engineering Laboratory, December 1995.

Thomas, H. M., "Pipe and Vessel Failure Probability," *Reliability Engineering, 2*, pp. 83-124, 1981.

10. HUMAN RELIABILITY ANALYSIS

The third element in a Level 1 probabilistic risk assessment (PRA) consists of data analysis, human reliability analysis (HRA), and the quantification and generation of results (refer to Figure 1.3). The objectives of the HRA task are to identify, analyze, and quantify human failure events (HFEs). These overall objectives can be clarified by considering two distinct cases:

1. Pre-Initiating Event HFEs. This task is to quantify pre-initiating event HFEs that were identified during the Systems Analysis task.

2. Post-Initiating Event HFEs. Many post-initiating event errors of omission will have been identified during the Event Sequence Modeling and Systems Analysis tasks. This task must extend that list and perform the following activities:

   - Identify the context associated with each identified HFE,
   - Quantify the chance of each HFE, i.e., the probability of the HFE given the defined context,
   - Identify and quantify the probability of human recovery for significant sequences, mindful of the dependent effects of unexpected plant conditions and unfavorable human performance conditions, i.e., the context for the human action.

Figure 10.1 shows the important relationships between the subtasks under HRA and the other major components of the PRA.

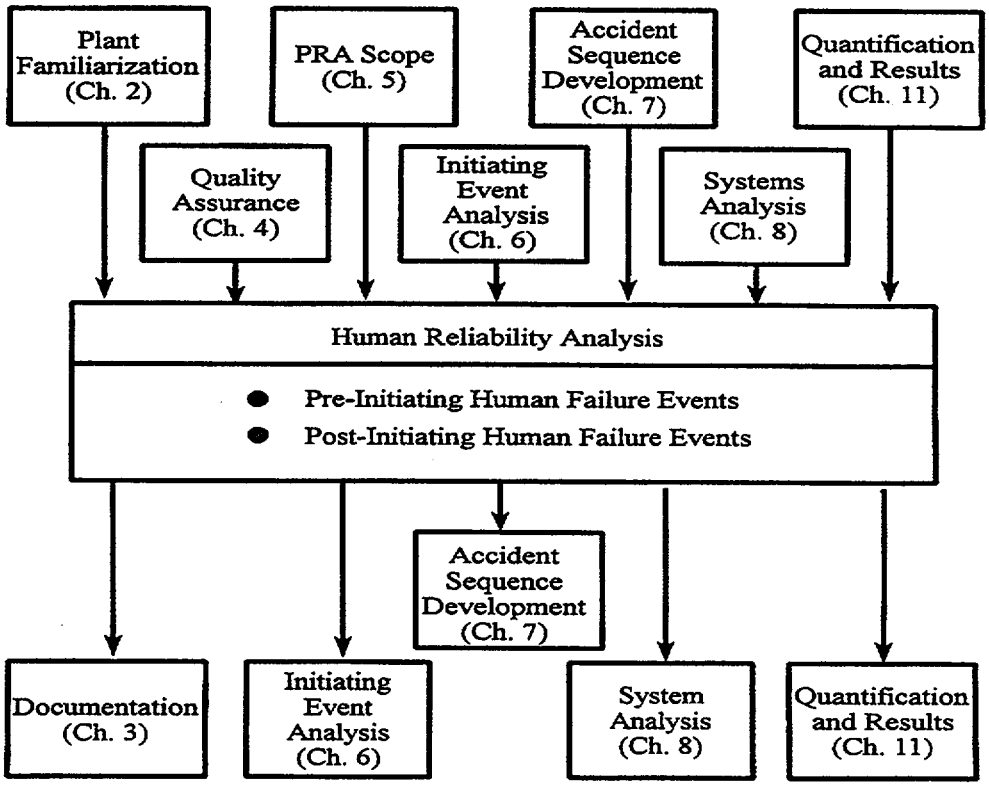


Figure 10.1 Relationships between human reliability analysis and other tasks

10.1 Relation to Other Tasks

This task has extensive interactions with the following other PRA tasks.

Plant Familiarization. The HRA relies on information from the Plant Familiarization task to provide a basic understanding of plant design, operations, procedures, and crew manning levels.

Initiating Event Analysis. Development of initiating events should take into account the HRA contributions.

Accident Sequence Development. The HRA relies on the Accident Sequence Development task to identify a number of post-initiating event HFEs, to describe how the plant can fail in an integrated sense, and to define the context under which the operators must act.

System Modeling. The HRA relies on the System Modeling task to identify pre-initiating event HFEs and a basic understanding of how systems are operated and are interrelated.

Quantification and Results. The Initial Quantification is used to identify specific cases (sequences and cutsets) where human recovery actions are likely to be carried out and impact the results. The HRA provides quantified HFEs to use in the quantification of specific cutsets in the Quantification tasks.

10.2 Task Activities

The primary discussion in this chapter deals with dynamic actions following the initiating event. A second class of actions, pre-accident errors that are generally associated with test and repair activities, can be important in two cases:

1. When post-maintenance testing is insufficient to ensure that tested or repaired equipment has been completely restored to service. In this context, insufficient testing means insufficient by lack of procedural quality, by lack of assurance that the test will be performed, or by lack of test procedures.

2. When pre-accident errors can cause or influence post-accident human response, i.e., through a dependency between the pre- and post-accident errors.

These types of errors can be modeled using the methods described in the "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications" (Swain and Guttmann, 1983), although the recommended values for human error probabilities cited will need to be verified as described below.

The post-initiating event HFEs (i.e., those occurring while attempting to mitigate the progression of the accident sequence) pose a much more complicated and risk-significant problem than the pre-initiating event kind. Since the human operators can interact with the plant and its processes in many ways, it would be impossible to precisely model all these potential interactions. Therefore, a structure is required to organize the analysis along the most fruitful and important lines. Traditional approaches to HRA, such as THERP and SLIM (e.g., Swain and Guttmann, 1983; Embry et al., 1984), focus on those actions known to be required for successful completion of functions modeled in the event trees, i.e., those HFEs that have been known as errors of omission. However, reviews of operating events at nuclear power plants and other industrial facilities have shown that errors of commission are often involved in the more serious accidents (Barriere et al., 1994; Barriere et al., 1995; Cooper, Luckas, and Wreathall, 1995; and Cooper et al., 1996). Moreover, the most serious accidents occur when conditions conspire to make human error very likely, i.e., when both unusual plant conditions and unfavorable human conditions [performance shaping factors (PSFs)] combine to create an error-forcing context (EFC). For such cases, the HRA problem changes from an attempt to evaluate the likelihood of random human error under nominal conditions (i.e., expected accident conditions) to one of evaluating the likelihood of the occurrence of EFCs as addressed in the new method ATHEANA (see Appendix F).

A limitation of all existing methods is that they are not structured to address the question of errors of commission or the search for possible EFC. A second limitation of existing methods is that these methods do not provide guidance for the identification and prioritization of HFEs (see Appendix G). Rather, the HFEs drop out of the

event tree analysis and quantification tasks. This leads to a lack of consistency in the specific human actions addressed in similar PRAs. Because of the importance of human errors in real-world accidents, it is necessary to propose a modification of existing methods to address these issues. This procedure guide assumes that recently developed search techniques for HFEs and EFCs in the ATHEANA methodology (Cooper et al., 1996 and Wreathall and Ramey-Smith, 1997) can be adapted to existing quantification approaches to enhance the value of the PRA.

It is important to recognize that the HRA process for U.S. reactors may not apply to Russian reactors. For example, the PSFs of training, staffing, responsibilities, cross training, and cultural impacts on thinking can be different. Therefore, the assumptions that are implicitly embedded in quantification for many existing methods, e.g., tables for quantification using the THERP methodology (Swain and Guttmann, 1983), will not apply to the HRA of Russian reactors. Therefore, while existing methods can be used to structure the problem of where human error can occur and be corrected, their quantification information is highly suspect. For the Russian PRA project, a structured judgment approach for quantification will be required. For the pre-initiating event HFEs, some modification to the quantification tables in the handbook (Swain and Guttmann, 1983) involving the judgment of Russian experts will be needed. For the post-initiating event HFEs, the Success Likelihood Index Method (SLIM) will be used (Embrey et al., 1984). It provides a structured approach for applying expert judgment based on the evaluation of PSFs for each HFE. The SLIM quantification can be enhanced by the thinking process of ATHEANA. This process entails evaluating the most-likely-to-be-significant HFE-EFC pairs, the likelihood of the occurrence of the EFC, and the likelihood of the HFE under the EFC. This judgment-based evaluation offers a better chance for reasonableness than a table lookup that is based on inapplicable experience.

This task is accomplished by completing five activities:

1. Quantification of pre-initiating event HFEs,
2. Development of a detailed list of post-initiating event HFEs,
3. Development of a detailed list of significant context associated with each post-initiating event HFE,
4. Quantification of post-initiating event HFEs,
5. Recovery analysis.

Each of these activities is discussed below, and the work products are summarized in Section 10.3. This approach represents an extension of the HRA methodology beyond that found in the IAEA procedure guides (IAEA, 1992). Activity 1 is a stand-alone task. The next three, Activities 2-4, are linked together as the step-by-step evaluation of the post-initiating event HFEs. These activities are closely related to other PRA tasks. Pre-initiating event human errors are identified in the task System Modeling. Post-initiating event human errors modeled in the fault trees and event trees are identified in the tasks System Modeling and Event Sequence Modeling. Recovery actions will be identified after completion of the initial quantification (see Section 11.1) and quantified in the final quantification (see Section 11.2). The ways the actions are included in the event trees and fault trees will be determined in coordination with the activities in System Modeling and Event Sequence Modeling. The quantification of these actions will allow System Modeling and Initial Quantification of Accident Sequences to proceed.

10.2.1 Activity 1 — Quantification of Pre-Initiating Event HFEs

Pre-initiating event errors may leave part (or all) of a system unavailable for emergency operation. These types of errors occur during routine plant operation, testing, and repair activities and may persist undetected before the occurrence of an initiating event. They are included only in the system fault trees for the following reasons:

- The error rates for these actions do not depend on the sequence of events after an initiating event occurs.
- There is generally no significant human dependence between these errors and subsequent operator actions after the initiating event occurs. (Note that the ATHEANA search for EFCs considers cases in which this assumption of independence may not be valid.)

These types of errors can contribute to system unavailability if all of the following conditions occur:

- A test, inspection, or repair activity is performed. During this activity, a component is placed in an alignment that makes it unavailable for emergency operation.
- Testing, repair, or operations personnel fail to restore the component to its required status.
- The faulty condition is not discovered and corrected before an initiating event occurs.

The general format for quantification of the unavailability contribution from these errors is shown by the following two expressions:

$$Q_{HET} = \lambda_T \phi_{HET} T_{DT}$$

and

$$Q_{HER} = \lambda_R \phi_{HER} T_{DR}$$

where Q_{HET} = Unavailability due to testing errors
λ_T = Testing frequency (test/hour)
ϕ_{HET} = Testing human error rate (error/test)
T_{DT} = Testing error mean detection time (hours/error)
Q_{HER} = Unavailability due to repair errors
λ_R = Repair frequency (repair event/hour)
ϕ_{HER} = Repair human error rate (error/repair event)
T_{DR} = Repair error mean detection time (hours/repair event).

This task proceeds by quantifying the human error rates for test and repair operations, λ_T and λ_R, that were defined in the task System Modeling. The methods found in the handbook (Swain and Guttmann, 1983) shall be followed, except that the tabulated error rates must be judgmentally adjusted for the Russian reactor plant environment.

10.2.2 Activity 2 — Development of a Detailed List of Post-Initiating Event HFEs

The human actions that are directed by plant procedures form the traditional basis for defining errors of omission for each initiating event. These HFEs are identified during the Accident Sequence Development task and verified with plant operators. The selection of HFEs has to be based on plant-specific design, capabilities, and priorities.

10.2.3 Activity 3 — Development of a Detailed List of Significant Context Associated with Each Post-Initiating Event HFE

The analysis of each HFE begins with a SLIM analysis (Embrey et al., 1984) that carefully accounts for the "normal" context defined by the scenarios detailed in the event trees. The context must include at least the following information and must be verified with plant operators.

1. Preceding Events. Describe the initiating event, any previous human actions, and special plant conditions (failed equipment, pipe breaks, etc.).
2. Indications of Plant Conditions. Describe what the crew actually can see; how long it could exist before diagnosis and the reasons for any possible delays, and all redundant indications.
3. Procedural Guidance. Provide details of the procedures that the crew would be expected to use and any procedures that could accidentally be used.
4. Training and Experience. Are the crews trained on this situation? How and when? Have they encountered similar situations in actual operations? Provide details.
5. Concurrent and Competing Factors. Describe expected alarms, environment,

other actions required by the scenario, and any other stressors.

6. Indications of Success. What plant indications will inform the operators of the success or failure of their actions?

7. Failure Impact. Describe the plant conditions following failure to complete this action. Is recovery possible?

8. Time Constraints. Thermal-hydraulic analysis may indicate that actual time available for this action. What is known about the time required for the operators to diagnose the current condition and carry out the action?

Examples of context descriptions at this level can be found in Chien et al. (1988) and Chu et al. (1994).

10.2.4 Activity 4 — Quantification of Post-Initiating Event HFEs

The SLIM approach will be used and is well described in its methods documentation (Embrey et al., 1984). Briefly, it involves five steps carried out by judges with expertise in the plant PRA, plant operations, SLIM, and cognitive performance.

1. Modeling and Specification of the PSFs. The judges review the task at hand and its context, performing a task analysis. They select the relevant PSFs, e.g., training, procedural guidance, and quality of indications.

2. Weighting the PSFs. One approach is to imagine a case where all PSFs are as bad as possible. Then select the single PSF that, if improved, would create the greatest improvement in the probability of success and assign that PSF a weight of 100. Then select the PSF with the next most impact on success and assign its weight as a fraction of the first. Repeat for all PSFs and rescale the weights by normalizing to 1.0. The weights indicate the relative importance of each PSF towards overall success.

3. Rating the Task. Rate each PSF on a scale of 0-100, where 0 means that the PSF is as bad as possible (in this scenario) and 100 means that it contributes to success as much as possible. The ratings indicate the judges evaluation of each PSF (independent of the others) in this particular scenarios over its possible range.

4. Calculate the success likelihood index as the sum of the products of weight x rating over the PSFs.

5. Convert the success likelihood index to probability of success, using calibration events based on experience, well-accepted analysis, or well-supported judgment.

10.2.5 Activity 5 — Recovery Analysis

The "recovery" analysis addresses additional human actions, not previously selected for analysis in Activity 2 and quantified in Activity 4, that appear to be important in preventing core damage following the initial quantification of the PRA.

To some extent, the activities of the previous two tasks included recovery analysis. Unlikely, but severe, context identified in previous cases precluded the opportunity for further recovery actions. However, in light of the existing analysis presented in this guide, recovery will be considered in the task Initial Quantification of Accident Sequences (for those sequences that include HFEs). The recovery analyses will document all PRA sequences for which recovery was considered, explaining the reasons why subsequent analysis of recovery actions was or was not conducted. In those instances where recovery actions were analyzed, the analysis will be documented, explicitly considering the effects of the original error-forcing context.

10.3 Products

The results of each pre-initiating event HFE analysis will be documented in a report as part of the Human Reliability Analysis appendix to the PRA Report in accordance with Chapter 3. This report will also detail the basis for directly using,

or modifying, the tables for quantification in the Swain and Guttmann (1983) handbook.

A detailed list of HFEs will be documented in a letter report. The search process for HFEs will consider the event tree model and those top events where human errors of omission or commission can defeat the associated safety function and make core damage likely.

An HRA report will be produced documenting Activities 1-4, providing the list of HFEs, detailing the context for each HFE, and documenting the SLIM process and quantification results. This product will become part of the Backup Documentation, Human Reliability Analysis.

A detailed list of normal context and significant EFCs associated with each HFE will be documented in a report. The search process for EFCs begins with the HFE, then identifies the most important EFCs in a stepwise process. This product will specify the HFE-EFC pairs identified for quantification and document the search process and associated analyst decisions. This letter report will become part of the Human Reliability Analysis appendix to the PRA Report in accordance with the instructions in Chapter 3.

The recovery analysis will document all PRA sequences for which recovery was considered, explaining the reasons why recovery was or was not analyzed, and, when analyzed, documenting the analysis, explicitly considering the effects of the context. This work will be documented in the Backup Documentation, Human Reliability Analysis, and for recovery events actually included in the PRA, as part of the Human Reliability Analysis appendix to the PRA Report in accordance with Chapter 3.

10.4 References

Barriere, M. T., et al., "Multidisciplinary Framework for Human Reliability Analysis with an Application to Errors of Commission and Dependencies," NUREG/CR-6265, Brookhaven National Laboratory, August 1995.

Barriere, M., et al.,"An Analysis of Operational Experience During Low Power and Shutdown and A Plan for Addressing Human Reliability Assessment Issues," NUREG/CR-6093, Brookhaven National Laboratory, June 1994.

Chien, S. H., et al., "Quantification of Human Error Rates Using a SLIM-Based Approach," Proceedings of the 1988 IEEE Fourth Conference on Human Factors and Power Plants, Monterey, California, June 1988.

Chu, T.-L., et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1: Analysis of Core Damage Frequency from Internal Events During Mid-Loop Operations," Vol. 2, Part 1B, Chapter 8, NUREG/CR-6144, Brookhaven National Laboratory, June 1994.

Cooper, S. E., et al., "A Technique for Human Error Analysis (ATHEANA): Technical Basis and Methodology Description," NUREG/CR-6350, Brookhaven National Laboratory, June 1996.

Cooper, S. E., W. J. Luckas, and J. Wreathall, "Human-System Event Classification Scheme (HSECS) Database Description," Brookhaven National Laboratory Technical Report L-2415/95-1, December 21, 1995.

Embrey, D. E., et al., "SLIM-Maud: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment," NUREG/CR-3518, Vols. 1 and 2, Brookhaven National Laboratory, 1984.

IAEA, "Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1)," Safety Series No. 50-P-4, International Atomic Energy Agency, 1992.

Swain, A. D., and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, Sandia National Laboratories, 1983.

Wreathall, J., and A. Ramey-Smith, "ATHEANA: A Technique for Human Error Analysis--An Overview of Its Methodological Basis," OECD/NEA Specialists Meeting on Human Performance in Operational Events, Chattanooga, Tennessee, October 13-17, 1997.

11. QUANTIFICATION AND RESULTS

The third element in a Level 1 probabilistic risk assessment (PRA) consists of data analysis, human reliability analysis, and the quantification and generation of results (refer to Figure 1.3). The quantification and results component consists of three tasks: (1) initial quantification of accident sequences, (2) final quantification of accident sequences, and (3) sensitivity and importance analyses. This is shown on the flowchart in Figure 11.1. The objective of the task on initial quantification is to perform an initial, preliminary quantification of the set of accident sequences, i.e., once the event tree-based, system-level expressions become available. Through this task, models that represent the response of plant systems and operation actions are linked to plant initiators to form, in terms of basic events, the logic expressions for accident sequences. The objective of the final quantification is to identify those accident sequences considered to be dominant after initial quantification and to determine where refinements to the risk profile may be warranted and then to carry out the new quantification. The objective of the sensitivity analysis is to investigate the implications of modeling choices other than the choices that were actually used. Importance analysis is to assess the importance of model parameters, evaluated within the terms of the model itself.

Figure 11.1 shows the important relationships between the tasks under quantification and results and the other major components of the PRA. These relationships are explored in more detail in each of the sections describing the three tasks. Initial quantification is discussed in Section 11.1, final quantification in Section 11.2, and sensitivity and importance analyses in Section 11.3.

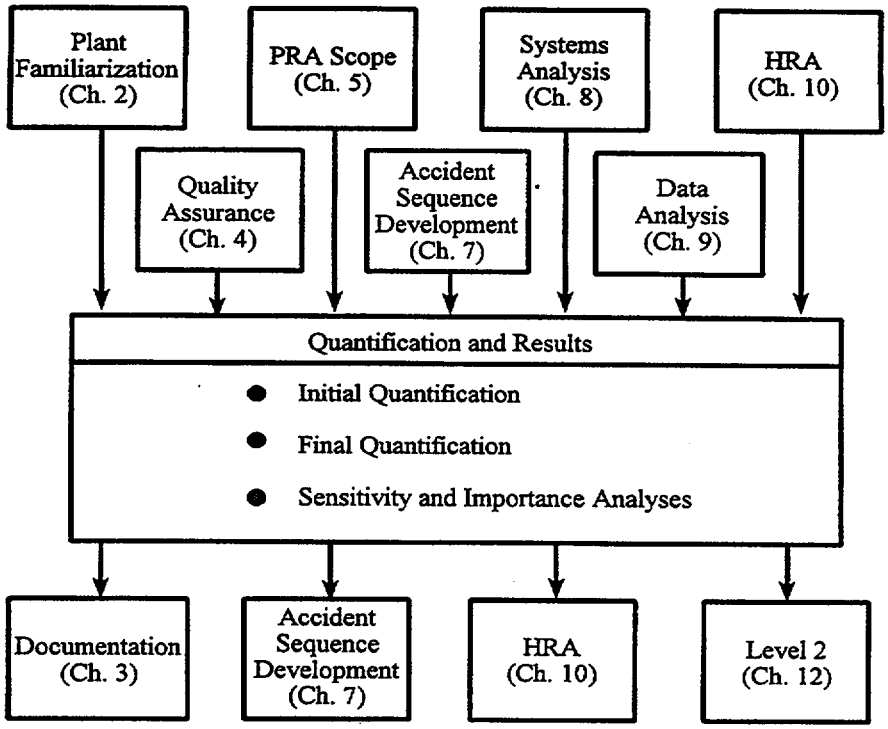


Figure 11.1 Relationships between quantification and results and other tasks

11.1 Initial Quantification of Accident Sequences

The objective of this task is to perform an initial, preliminary quantification of the set of accident sequences, i.e., once the event tree-based, system-level expressions become available. Through this task, models that represent the response of plant systems and operator actions are linked to plant initiators to form in terms of basic events the logic expressions for accident sequences. Initial quantification is described below in general terms. More detailed guidance is provided in some of the references listed at the end of this chapter. In particular, reference should be made to Drouin (1987) and NRC (1997).

11.1.1 Relation to Other Tasks

As indicated in Figure 11.1, the Initial Quantification task has extensive interactions with other PRA tasks:

Quality Assurance. The Initial Quantification task has obvious interfaces with QA requirements.

All Internal Event Analytical Tasks. This task is the first attempt to integrate all previous work, especially all of the individual system models, into one consistent model whose framework was developed in the event sequence modeling. As a practical matter, this task also requires at least preliminary data, which emerge from assessment of human reliability and component reliability. Although described here as a single task, Initial Quantification of Accident Sequences is part of an iterative process involving all previous tasks. In carrying out this task, it is generally necessary to approximate ("truncate") the sequence expressions, and this approximation is generally controlled through the quantification process. The proper modeling of each system conditional on the states of other systems is revisited as the preliminary sequence results become available. Iterating between the sequence models and the system-level models takes place during this task to assure proper conditionality between systems and to search for logic errors in sequence cutsets. Based on this preliminary quantification, priorities are to be reviewed, and additional modeling or data refinement needs are assessed. In a subsequent task, leading contributors to sequence frequencies are analyzed further to see whether recovery modeling changes the results significantly. If so, the sequence expressions are augmented to reflect recovery.

11.1.2 Task Activities

Compromises and assumptions that were made in previous tasks, such as the event sequence modeling task, the system modeling task, and data analysis task, indirectly limit the output from this task. Further limits on the applicability of the outputs from this task directly come from the limits imposed by the level of truncation employed and the lack of recovery modeling employed in the model. Since the output from this task is based on preliminary data and partial modeling (recovery is addressed in a subsequent task), the information derived should only be applied to prioritize future work. The following activities are performed as part of this task.

11.1.2.1 Activity 1 — Boolean Expressions

Initiate an algorithm that transforms each system-level accident sequence representation derived from the task Event Sequence Modeling into a component-level, Boolean expression containing the minimal cutsets.

11.1.2.2 Activity 2 — System Success

Account for system success as necessary by using the approximation techniques mentioned below.

11.1.2.3 Activity 3 — Truncation Levels

Re-run the calculation with different truncation levels until the calculation runs to completion with as little truncation as possible. Of course, the level of the truncation should be commensurate with the intended application of the PRA study and the level of available data. Identification of potential subtle interactions between systems and support systems requires, for example, retention of higher order cutsets.

11.1.2.4 Activity 4 — Plant Damage States

Formulate and quantify a logic expression for each plant damage state (corresponding to the logical OR of sequences binned into that state).

11.1.2.5 Additional Guidance

Model Integration

Since the process described above is the integration of a large amount of information for the first time, a significant level of review, troubleshooting, and iteration with previous tasks is necessary. An accident sequence expression can be very complex, and subtle logic errors manifest themselves at this stage. Incorrect formulations, in the context of a system model, may lead to erroneous logic at the sequence level. Disallowed system configurations that have been eliminated from system models may emerge again at the sequence level, depending on how disallowed configurations have been dealt with.

Conditional Relationships Between Events

Much of the point of the detailed model development is to properly reflect the conditional relationships between failures of different systems or between the initiating event and subsequent system failures. For example, if a support system failure affects more than one system in a sequence, this is likely to be important, and it is essential for this to be properly reflected in the accident sequence expression. Similarly, if a pipe break initiating event can adversely affect mitigating systems, this must be captured. In order for these properties to hold, the linkage must be modeled properly, and the sequence quantification task must be executed properly. Although the project controls in the system modeling task should have ensured that the separate system models are properly interfaced, review at this stage to see that it has been done properly is a good idea. This interface activity is more fully addressed under the task Quality Assurance (refer to Chapter 4).

System success in a sequence may also be significant. The conjunction of system A succeeding and system B failing may be much less likely than the unconditional failure of system B viewed in isolation. It has been found that neglect of this point can seriously distort accident sequence quantification. Therefore, it is customary to address this point, even though neglecting it may be "conservative" and addressing it is troublesome. Formally, one should construct an expression which logically ANDs system A success with system B failure. The feasibility of this will depend on many things, including the software being used. It has been customary to address this point by formulating a logic expression containing the conjunctions of failures that are considered inconsistent with the sequence logic (success of system A and failure of system B). This logic expression is then used as a template to systematically delete from the pure failure portion of the accident sequence expression those terms indicated by the template to imply the failure of the system that is supposed to succeed. At best, this is an approximation and, in applying it, one must take care not to eliminate "late" system failures that may be consistent with "early" system success. This point is further discussed below.

So-called "phased mission analysis" is very closely related to this point. A particular system may be challenged more than once during an accident sequence, perhaps with different mission success criteria. The system modeling must accommodate the necessary distinctions, but this point is not completely addressed until accident sequence quantification. Certain illogical outcomes must be avoided. A contribution that implies early failure and late success may be an error. Contributing factors are that the failed equipment is either restored (and the restoration is modeled) or that mission success is indeed compatible with both early failure and late success. The situation is more complex with respect to early success and late failure. There may be contributions to late failure from system failures occurring after the early success that are not necessarily incompatible. However, care must be taken. Exhaustive treatment of these issues is not common in U.S. full power PRAs, partly because it is burdensome and not necessarily important (see, for example, Drouin, 1987). It appears in many full power PRAs that failures occurring during standby are much more important than failures occurring after an initiating event (because the exposure time is much longer). However, it is the analyst's burden to address these issues and decide whether it is

necessary to allocate modeling resources to them. In general, a conservative approximation will present itself, and this can be adopted if it does not distort the risk profile in an unacceptably misleading way. A paper by Xue and Wang (1989) discusses the issues and presents algorithms to include during sequence quantification.

Truncation

Obtaining explicit, reduced, complete, basic event level expressions for all accident sequences would be impracticable for most plant models developed in recent years. The Boolean expressions become too large to be manipulated efficiently. (The large event tree approach may offer certain advantages in this regard.) However, the top event frequency may be dominated probabilistically by a small fraction of the terms in the full expression. Many terms can then be neglected without significant change to the results or conclusions. The process of "truncating" these contributions makes accident sequence quantification feasible. Typically, this is implemented in a computer code by setting a truncation cutoff level and instructing the algorithm to dispose of cutsets whose probability is less than the cutoff. The effect of such an algorithm is not always easy to predict; for example, it can depend on the level of detail to which failure events have been modeled. If a failure event has been decomposed into a large number of individually unlikely basic events, then cutsets containing these unlikely events are more likely to be truncated than if a single lumped event is used to capture all of the contributions.

If truncation is done without an appreciation of how much top event probability is being sacrificed, then it is an uncontrolled approximation. This is an important point. It is customary to base many sensitivity studies and importance analyses on the Boolean expressions obtained through the truncation process. Clearly, the results of such sensitivity studies can be seriously distorted by truncation. Truncation is, therefore, to be carried out only to the degree necessary to allow the analysis to go forward in a practical way, and its effects on later uses of the results must be assessed.

Evidently, if a sequence's probability (conditional on the initiating event) is assessed to be only a few orders of magnitude greater than the truncation level used to simplify processing, then the result is clearly suspect.

11.1.3 Products

1. Based on unrefined data, screening human error probabilities, and taking no credit for recovery, this task produces reduced logic expressions and associated frequencies for each accident sequence and each plant damage state.

2. In addition, although this task does not produce final results, it must be documented to the degree necessary to support an audit of the subsequent modeling choices that were based on the results of this task. In particular, it should be documented sufficiently to support replication of the results. This documentation will take the form of an appendix, as described under the task Documentation. The types of PRA audits are discussed in the task Quality Assurance.

11.2 Final Quantification of Accident Sequences

At this stage of the analysis, certain portions of the model may have been constructed in a simple way with a slightly conservative bias in order to obtain a "quick look" at the risk profile. The objective of this task is to identify those accident sequences considered to be dominant at this stage of the analysis and to determine where refinements to the risk profile may be warranted. Two such areas where refinements are necessary are human error modeling and parametric common-cause modeling. Other areas may have been treated similarly by the analysts. At this stage, sensitivity of results to each issue is assessed to determine whether more work is necessary to improve the model in this regard. As indicated in Section 11.1, more detailed guidance on this task is provided in some of the references at the end of this chapter.

Until preliminary sequence models were available, recovery modeling was somewhat premature. At this point, leading contributors to sequence frequencies are further analyzed to see whether recovery modeling changes the results significantly. If so, the sequence expressions are augmented to more fully address operator/plant recovery actions.

"Quantification" implies treatment of uncertainty. For purposes of this task, uncertainty of each model parameter is developed as appropriate in the tasks on human reliability analysis, component reliability, or common-cause failure probabilities. The propagation of parameter distributions through the integrated model is accomplished by software whose detailed description is beyond the scope of this guide. Ericson et al. (1990) does provide some information regarding software used for uncertainty propagation.

11.2.1 Relation to Other Tasks

As indicated in Figure 11.1, the Final Quantification task has extensive interactions with other PRA tasks as indicated below:

Quality Assurance and Documentation. The Initial Quantification task has obvious interfaces with QA requirements and provides input to the PRA documentation.

All Internal Events Analytical Tasks. This task integrates the results of all previous analysis tasks after they have been refined during the Initial Quantification of Accident Sequences (Section 11.1 above). It is assumed that debugging has been done as part of the initial accident sequence quantification task.

Level 2/3 Analyses. Output from the Final Quantification task provides information on accident sequence definition and on frequency of occurrence directly to the Level 2 task (refer to Chapter 15) which in turn provides source term information to the consequence and risk integration task (refer to Chapter 16). Whether or not Level 2/3 analyses are performed depends on the scope of the PRA (refer to Chapter 5).

11.2.2 Task Activities

Most of the parameters that appear explicitly in a PRA model are not objective physical parameters. Rather, they are frequencies or split fractions that depend on manufacturing processes, programmatic activities, management decisions, maintenance practices, operator training, and so on. When a PRA model has been refined to where the results are considered state of knowledge and when the PRA model provides a representative picture of the as-built, as-operated plant, then a key output of the overall project is the body of embedded assumptions upon which the model structure and model parameters rest. The technical adequacy of the PRA is closely aligned to how well these assumptions are fulfilled.

This point is discussed further in the section on Sensitivity and Importance Analyses.

11.2.2.1 Activity 1 — Sensitivity and Uncertainty

Sensitivity and uncertainty analyses are carried out to ascertain contributors that are dominant to the risk profile and contributors that are not dominant but to which results are sensitive. This activity should be done generically, either with emphasis on human errors or with emphasis on common-cause parameters and, also generally, with a view toward deciding which areas may need attention. The analysts should begin by simply looking at the minimal cutsets to see what is dominant. Computer-assisted analysis can help in this regard. Some items whose "point" likelihood seems small may actually dominate the results when uncertainty is properly reflected, and this is the kind of item that needs more attention.

11.2.2.2 Activity 2 — Enhanced Modeling

Uncertain probabilities may have been conservatively quantified in the initial quantification in order to prevent possible loss of significant scenarios in a screening process. Therefore, at the present stage, items that appear insignificant are likely to be insignificant, unless there is significant uncertainty associated with them. Decisions are made at this stage as to whether sensitivity items have been modeled well

enough and, if not, how the modeling should be enhanced.

11.2.2.3 Activity 3 — Recovery Actions

Significant recovery actions are identified, and engineering descriptions of these actions are furnished to the analysts responsible for their quantification. These are actions for which credit can be justified and for which results are significantly altered. These actions may include those actions performed in direct response to an accident and/or actions performed in recovering a failed or unavailable system or component. Credit for both types of actions should not be taken unless procedural guidance and training in the required actions are part of the operations at the plant.

11.2.2.4 Activity 4 — Requantification

The entire model is requantified using the best available models and data. Propagation of uncertainty through all models is included in this activity. Software for propagating uncertainty distributions are available and are mentioned in the Ericson et al. reference, for example.

11.2.2.5 Additional Guidance

Common-Cause Modeling

Based on the preliminary accident sequence quantification and on sensitivity and importance results, the common-cause quantification is reviewed (see Section 9.3), and the resulting parameterization is used in this task.

Recovery Modeling

In many plants, particularly older ones, it has been found that unacceptable results (unacceptably high accident frequencies) are obtained if it is assumed that no operator action is taken to initiate or reinitiate system operation in the event of problems, such as misaligned valves or breakers, spurious system trips, or even outright component failure. It is, therefore, necessary to model actions taken after the initiating event, not only the proceduralized actions represented at the event tree heading level but also actions that could potentially be taken to recover failed equipment. Correspondingly, appreciation of the role of these actions in the safety basis has been significantly enhanced, possibly through the development or revision of emergency operating procedures and other procedural guidance and operator training.

Such recovery actions must, in general, be modeled at or near the cutset level rather than at the system level. Recoverability of a system depends on which component has failed and on the environment near the failed component that could jeopardize recovery actions by operators. There are other factors as well. Is the component accessible? Is the environment too harsh, or even contaminated? How much time will be needed to effect any necessary repair? The answers to these questions depend, in general, on the details of each particular cutset. At the very least, recoverability depends on the basic event being analyzed. More generally, however, recoverability (even "diagnosability") of each event depends on the state of the rest of the system.

As such, everything that is true for the accident sequence is true for every minimal cutset in the sequence. In addition, each minimal cutset has more specific characteristics that must be accounted for.

Modeling of any particular instance of "failure to recover from a basic event" is, of course, a particular application of human performance modeling. Techniques to accomplish this are discussed in the task Human Reliability Analysis. These techniques do not come into play until the scope and feasibility of each recovery action have been established from an engineering point of view.

Occurrence of a particular basic event may essentially place a system into an irreversible state from which recovery of the basic event does not recover the system, even though no minimal cutset is strictly true with the event recovered. A trivial example would be an event, such as loss of seal cooling, that leads to a transient-induced loss-of-coolant accident. Recovery of cooling will not necessarily reseal the loss-of-coolant accident. In addition to these types of cases in which one component suffers damage as a result of another's behavior, it is possible for other kinds of state changes to occur that are not necessarily

unrecoverable but whose recovery must be analyzed in the context of the entire cutset.

Since each accident sequence may comprise thousands of minimal cutsets, it may be asked how feasible is it to approach recovery modeling with any rigor at the cutset level. Fortunately, some of the above considerations can be formulated logically within some software packages, permitting some automation of the process of recovery modeling. This kind of modeling has been very important in the analysis of older U.S. plants.

Guidelines for Prioritization

In order to produce the best possible final result, it is important to identify those areas of the model that need the most work.

Some rules of thumb for evaluating individual systems or components are listed here. It is reemphasized that the analysts are responsible for formulating and applying their own reasoning processes.

Items (systems or basic events) that have a high Fussell-Vesely importance (or high Risk Reduction Worth) are candidates for reexamination because the overall results are clearly sensitive to these items. If they were improved (e.g., increase in system availability), the calculated risk would diminish. If the quantification upon reexamination is found to be reasonable, then cost-beneficial ways to reduce these contributions should be considered.

Items that have a high Birnbaum importance (or high Risk Achievement Worth) are also candidates for examination because they are frequently challenged. If they have a high Birnbaum importance and a low Fussell-Vesely importance, this is because they have been modeled as very reliable. The results of the model depend critically on the correctness of this modeling, and it is important to make sure that the items are truly reliable.

Items that have both high Fussell-Vesely and high Birnbaum importances should be examined very carefully. Such items are challenged frequently, but they are not considered reliable. These items are high priority items.

All of the above comments are affected by uncertainty.

The single-event importance measures on which the above rules of thumb are based have very limited meaning. Events that are "important" can be considered to need examination, but generally, unless a model contains significant single-failure cutsets, combinations of events are more important than individual events, and the single-event importance measures are a poor way to analyze combinations. In a related vein, the effects of embedded assumptions are potentially very important. A marginal success path credited in the PRA can artificially and inappropriately reduce many single-event importances. These matters are discussed further under Sensitivity and Importance Analyses.

11.2.3 Products

The products for this task are the expressions, probability of frequency plots, and associated mean frequencies for: (a) each accident sequence, before and after recovery is credited and (b) each plant damage state, before and after recovery is credited.

11.3 Sensitivity and Importance Analyses

There are two major objectives of this task. One objective ("Sensitivity Analysis") is to investigate the implications of modeling choices other than the choices that were actually made in the formulation of the model. This is necessary in order to reinforce the credibility of the model and, by implication, the credibility of the safety basis. The other objective ("Importance Analysis") is to assess the importance of model parameters, evaluated within the terms of the model itself. This is done during modeling tasks in order to help focus resources on the most critical modeling areas and is done at the conclusion of the analysis in order to help in implementation of the safety basis (e.g., optimal allocation of testing and maintenance resources, based in part on measures of the importance of particular failure probabilities or particular maintenance unavailabilities).

11.3.1 Relation to Other Tasks

During model development, all of the major task activities will be performed iteratively; sensitivity and importance analyses are performed using the model available at the time to prioritize the resources. After completion of the model development, sensitivity and importance analyses are performed to evaluate the impacts of alternative assumptions and changes in plant design and operations on plant risks.

The following discussion reflects the logical hierarchy rather than the time ordering of the tasks. Sensitivity analysis is discussed first because its outcome has the potential to change the way in which the modeling is conducted. Importance analysis is discussed second.

Tasks whose outputs are candidates for sensitivity studies include the following:

- Initiating Event Analysis (formulation of the model can be sensitive to this),
- Functional Analysis and Systems Success Criteria (changing success assumptions can have major impacts), and
- System Modeling.

Tasks during which importance analysis is especially beneficial include the following:

- Common-Cause Failure Probabilities (effort allocated to quantification of common-cause model parameters should be a function of how important these parameters are, in the sense discussed below),
- Initial Quantification of Accident Sequences, and
- Final Quantification of Accident Sequences.

When all of the quantification tasks are substantially complete, importance results should be generated comprehensively and systematically in order to support the discussion of insights generated for the final documentation. In addition, sensitivity calculations can be performed to evaluate the risk impact of design improvements and alternative modeling assumptions. In some simple cases, sensitivity calculations can be performed using the importance results.

11.3.2 Task Activities

11.3.2.1 Sensitivity Analysis

In developing a Level 1 PRA model, many issues may arise due to lack of knowledge about them. For example, the success criteria for systems in different boundary conditions may be unknown, and the level of detail of a system model may need to be determined. One way to resolve the issue on success criteria is to perform detailed deterministic analysis including testing and experiments. In this case, sensitivity calculations can possibly determine the most important cases that should be deterministically evaluated. In the case of system modeling, sensitivity calculations based on a simplified logic model can potentially determine that a more detailed model is not necessary. PRA areas that are prime candidates for sensitivity analysis include: failure data, human reliability analysis, common-cause failure analysis, success criteria, and pump seal models.

Likely examples of highly significant issues are the feasibility of a particular recovery action taking place during an accident or a question of event tree structure (whether a given core damage sequence can be transformed into a successful outcome by operation of a particular system) or perhaps a question of binning (whether the phenomenology of a particular sequence warrants placing it into one bin or another).

If the sensitivity issue is such that extensive modeling would have to be undertaken in order to treat each possible outcome thoroughly and if such treatment is infeasible within the scope of the project, then it may be necessary to live with significant uncertainty in the results. Such an outcome is a rational input to consideration of follow-on work.

Particularly important instances of sensitivity calculations are those that establish the robustness of the mission success criteria assumed in the system models. These success criteria can significantly affect the logic structure of the model. Similarly, assumptions might have been made regarding whether certain transients cause safety relief valves to lift, and this can

affect event tree structure. It must be the responsibility of the analysts to identify priorities in these areas.

After the base case PRA model is finalized, the PRA can be used in different applications. Sensitivity calculations are often performed to evaluate the changes in plant risk as a result of changes in plant design, operation, and operator training. The changes at the plant may be to correct the vulnerabilities identified in the PRA study or to implement changes in regulatory requirements. For example, as part of the Individual Plant Examination program of U.S. plants, the utilities are required to perform sensitivity calculations to evaluate any plant improvements made as a result of the Individual Plant Examination. Other PRA applications include changes in allowed outage times in the Technical Specifications, increases in test or inspection intervals of the inservice testing program and inservice inspection program, and planning of online maintenance activities.

11.3.2.2 Importance Analysis

This section refers to importance analyses performed on sequence-level Boolean expressions.

When the plant model has been brought to a stage at which accident sequences are expressed in terms of trains and components (with component failures in support systems explicitly factored in), then a great deal of information is present in these sequence-level expressions. Some conclusions may suggest themselves from inspection of the expressions, but generally, their complexity make it impractical to try to derive insights in this way. At this stage, it is potentially useful to perform importance calculations which rank model parameters (such as basic event probabilities) according to how much the model parameter influences the results or how much change in the results would take place if the parameters were to change. These results are useful in deciding how much work to invest in carefully quantifying model parameters. In more advanced applications, one can assess the importance of conjunctions of events; the importance of a conjunction can help to decide whether to invest in searching for dependencies between the elements of the conjunction. When the PRA is substantially complete and the safety basis has been formulated, the importance analysis can help to establish how to allocate performance over the elements of the safety basis and, in particular, how to allocate testing and maintenance effort over the elements of the safety basis.

Finally, once the model has been brought into essentially final form, the importance analysis is the primary tool for deriving "insights" from the PRA. Importance information transcends the complexity of a plant logic model to provide a kind of sensitivity-type information that is understandable and can be very valuable. For example, in many previous studies, the top event frequency has been found to be dominated by a few contributors. That is, it has been found that scenarios that have in common relatively few "important" events sum to a large fraction of calculated top event frequency. A finding of this kind is important to discuss in the conclusions of the PRA. The reasons for such a circumstance should be identified and discussed.

At various stages of model development (cf. "relationship to other tasks" above), it is useful to develop importance ranking tables as part of a model review and debugging effort. It is first important to review the leading terms in the logic expressions for the various accident sequences in order to ensure that they make sense, but, in general, these expressions are too large to be reviewed entirely by inspection. Importance rankings by their nature provide information about the entire expression (information that must be interpreted with great care). Events at the top of the lists should be questioned: why are these events ranked highly? If the answer is not obvious, then the modeling should be checked, both in the logic aspects and in the quantification aspects. An analogous question should be asked about events at the bottom of the lists: why are these events ranked low? Again, if the answer is not obvious, then the model should be checked. Generally, surprises on the importance lists are either indications of modeling error or signal the emergence of a modeling insight. Events at the top of one or more importance lists need to be quantified with great care. Events appearing at the top of lists based on different measures should be examined with great care; such a case may correspond to a critical function being

unreliably performed. This would clearly warrant attention, both in modeling and perhaps in plant operation.

Background material on importance measures is furnished as Appendix H. There are some applications for which importance measures are not suited. Generally, if conventional importance analysis suggests that a particular system, structure, and component (SSC) is important, then it probably is; if conventional importance analysis suggests that a particular SSC is not important, this conclusion cannot be accepted without careful exploration of the reason for that result. Conclusions from importance tables are, therefore, to be drawn very carefully. During model development, however, importance analysis is a very useful way to develop understanding of the model.

The activities to be done for the importance analysis are:

1. In support of the Human Reliability Analysis (see Chapter 10), generate importance rankings for human errors (Fussell-Vesely and Birnbaum and/or Risk Reduction and Risk Achievement Worths).

2. In support of the parametric common-cause analysis (see Section 9.3), generate importance rankings for common-cause events (Fussell-Vesely and Birnbaum and/or Risk Reduction and Risk Achievement Worths).

3. Generate Fussell-Vesely importances for frontline systems.

4. When modeling is complete, generate final versions of the above to support the discussions of the PRA insights in the final report (see Chapter 3).

11.3.2.3 An Alternative Model to Sensitivity Analysis

Two approaches to resolving a modeling issue without performing extensive deterministic evaluation can be identified:

1. Based on the best judgment of the analyst, one modeling assumption is adopted as a base case, and other assumptions are evaluated in a sensitivity study.

2. Probabilistic weights, representing degree of belief in each assumption, are assigned to all possible assumptions and used with the logic models based on the assumptions.

In a Bayesian approach, such weights can be updated using any additional information that becomes available in the future.

Approach 1 represents the practice of a typical PRA. Approach 2 represents an improved approach which specifically address the "sensitivity" of the issue to alternative assumptions but requires more extensive effort. It has been successfully applied in the NUREG-1150 study (NRC, 1990) to some of the issues in severe accident modeling where extensive expert opinion elicitation was performed. Its NUREG-1150 application to Level 1 PRA issues is more limited in scope.

11.3.2.4 Limitations of Importance Measures

Single-event importance measures are sometimes presented as if they were capable of ranking model parameters in an objective way. However, no single model parameter can be ranked in isolation; the significance of each parameter depends in general on the model structure and on the values of all the other parameters. There are, of course, many other parameters, and it is correspondingly infeasible to analyze sensitivity to all combinations of variations of all parameters. All "sensitivity" results (chiefly importance measures of one kind or another) must be interpreted in light of this fundamental limitation.

Particular instances of these limitations are:

- Failure modes that are not modeled cannot emerge as "significant" from conventional importance analysis.

- For any given model parameter, the associated importance measures are

calculated conditional on all other model parameters behaving essentially nominally.

- Within the linked fault tree approach, the importance measures are calculated from a truncated model (truncated collection of minimal cutsets) and are correspondingly limited.

These points show that conclusions based on importance measures must be weighted in light of how the importance measures were calculated. A given item may show up as "unimportant" because it is logically in parallel with several other items (which can, therefore, compensate for its failure). Unfortunately, these other items are likely to show up as unimportant for the same reason, meaning that none of the SSCs in parallel is "important." It is possible for none of the SSCs in a critical function to show up as "important" in tables calculated in the usual way.

The users of these importance measures have to understand their definitions and limitations. Some of the shortcomings can be addressed with additional sensitivity calculations. For example, a lower truncation limit can be used to determine the sensitivity of the importance measures. The joined importance of groups of components can also be calculated. Relaxing requirements for those components that are individually ranked low should be further justified by demonstrating that the combined risk impact would also be low.

11.3.3 Products

The task produces the following:

- Importance rankings for systems and components at the conclusion of the study,
- Quantification of model sensitivity to alternative choices in controversial modeling areas (e.g., core damage frequency calculated assuming changes in baseline assumptions),
- System-level and component-level importance measures based on focused PRA model,
- Discussion of "PRA Insights" based on system and component importance measures.

11.4 References

Drouin, M., D., et al., "Analysis of Core Damage Frequency from Internal Events: Methodology Guidelines," NUREG/CR-4550, Volume 1, September 1987.

Ericson, D., et al., "Analysis of Core Damage Frequency: Internal Events Methodology," NUREG/CR-4550, Vol. 1, Rev. 1, Sandia National Laboratories, 1990.

NRC, "The Use of PRA in Risk-Informed Applications," NUREG-1602, Draft Report for Comment, June 1997.

NRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, U.S. Nuclear Regulatory Commission, December 1990.

NRC, "PRA Procedure Guides: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, U.S. Nuclear Regulatory Commission, January 1983.

Xue, D. and X. Wang, "A Practical Approach for Phased Mission Analysis," *Reliability Engineering and System Safety, 25,* 333, 1989.

PART D - OTHER EVENTS - LEVEL 1 GUIDELINES

12. FIRE ANALYSIS

The analytical tasks associated with a Level 1 probabilistic risk assessment (PRA) for accidents initiated by events internal to the plant (such as transients and loss-of-coolant accidents) are described in previous chapters. Other events both internal and external to the plant can cause unique initiating events or influence the way in which a plant responds to an accident. Figure 1.4 in Chapter 1 identifies three types of events (i.e., internal fires, internal floods, and seismic events) that require manipulation of the Level 1 internal event PRA in order to adequately model the plant response.

In this chapter, the way in which a Level 1 PRA is modified in order to model accidents initiated by internal fires is described. Figure 12.1 shows the important relationships between this task and other major tasks of the PRA. These relationships are discussed below in Section 12.1.

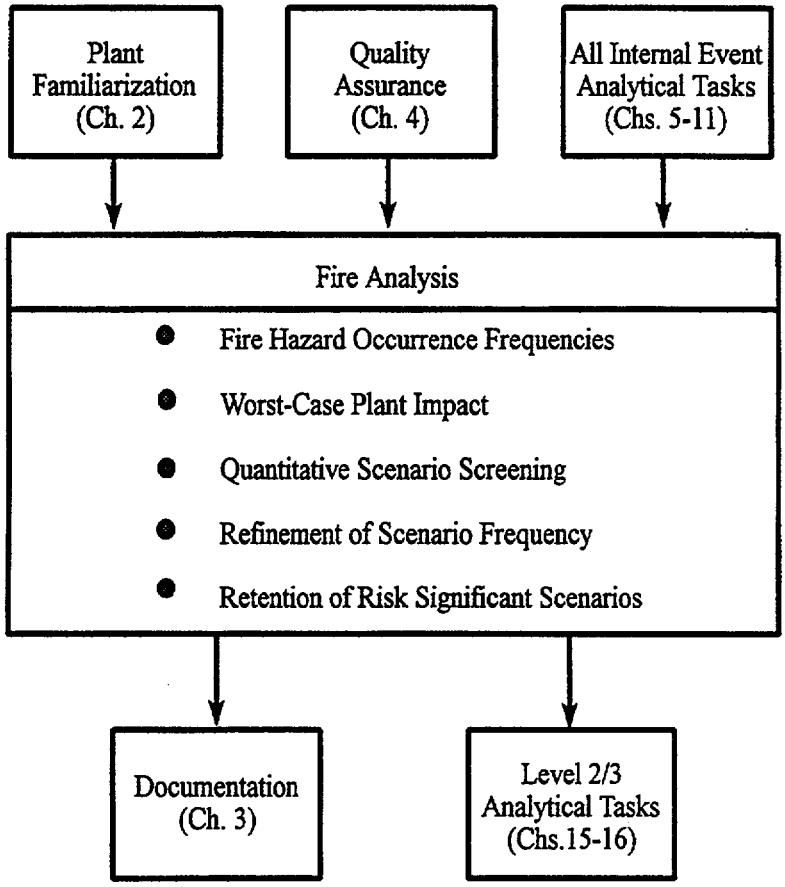


Figure 12.1 Relationships between fire analysis and other tasks

12.1 Relation to Other Tasks

As indicated in Figure 12.1, the Fire Analysis task has extensive interactions with all other PRA tasks:

Quality Assurance and Documentation. The Fire Analysis task has obvious interfaces with QA requirements and provides input to the PRA documentation.

All Internal Event Analytical Tasks. The current task utilizes the same overall analysis approach and procedures developed for the internal event PRA. In particular, this task builds on the information developed in the task Spatial Interactions (Section 8.3). The conduct of this task will require input from the tasks dealing with Initiating Event Analysis (Chapter 6), Frequency of Initiating Events (Section 9.1), Event Sequence Modeling (Section 7.3), and System Modeling

(Section 8.1). It is also likely that specific operator actions will be identified in the fire scenarios, thus prompting an interface with the task Human Reliability Analysis (Chapter 10).

Level 2/3 Analyses. Output from the Fire Analysis task provides information on accident sequence definition and on frequency of occurrence directly to the Level 2 task (refer to Chapter 15) which in turn provides source term information to the consequence and risk integration task (refer to Chapter 16). Whether or not Level 2/3 analyses are performed depends on the scope of the PRA (refer to Chapter 5).

12.2 Task Activities

A full power internal fire PRA utilizes the same overall analysis approach and procedures used in performing a full power traditional internal events PRA (Chapters 6-11). In fact, there are many points of commonality between the traditional internal events analysis and an internal fire risk analysis. These include the use of the same fundamental plant systems models (event trees and fault trees), similar treatment for random failures and equipment unavailability factors, similar methods of overall risk and uncertainty quantification, and similar methods for the plant recovery and human factors analysis. Consistency of treatment of these commonalities is an important feature in a fire risk analysis. Although the overall evaluation process is the same, there are differences in the events postulated to occur in response to an internal fire event as compared to those from a traditional internal event. These differences are described below in general terms. More detailed guidance can be found in NRC (1997) and Bohn (1990).

When preparing this chapter, some assumptions and limitations were made as indicated below:

- It is assumed that fire incidence data from VVERs are available. The fire data should be of sufficient resolution to allow categorization according to fire source (e.g., cable, switchgear, logic cabinet, etc.). If data are not available, or are incomplete, expert knowledge can be utilized.
- The approach outlined for treating the possibility of damage to electric cables due to fire assumes that cable function and routing information are known. If this is not the case, alternative approaches are available to address this type of damage. These alternative approaches will tend to be more conservative and overstate the contribution to core damage due to fire. One such alternative would be to assume that if a fire damages a cable of a given division, then all equipment in that division is assumed to be unavailable. Refinements to that alternative approach are, of course, possible if limited cable routing and function information are known.
- A simple and straightforward treatment of "hot shorts" and open circuits in control circuits is outlined herein. This approach, which does not treat the time dependence of circuit damage modes in a sophisticated manner, is assumed to adequately and conservatively represent the functional impact from these damage phenomena.
- This investigation has a characteristic approach that can be described as an "iterative conservative screening" of scenarios. The approach is to successively relax the most significant worst-case assumptions of each fire-initiated scenario and re-evaluate the impact of the fire on plant performance. Detailed phenomenological fire growth analyses found in such computer codes as COMPBRN (Ho et al., 1991) are typically of secondary importance for assessing the overall impact of fire hazards. Through conservative screening, there might be a few scenarios which may warrant the use of these types of detailed analyses in support of a typical fire PRA. It is assumed that a reasonable and practical quantitative screening criterion can be developed that would facilitate the completion of this task with minimal use of complex fire modeling codes.

- It should also be noted that these guidelines closely parallel those needed to perform the task Flood Analysis. Although these guidelines might seem to duplicate those found in the task Flood Analysis, individual procedure guides have been developed since different analysts are presumed to perform these tasks separately.

The specific goals of this task include the development of a fire frequency database, the determination of the frequency of specific fire scenarios, the further development and refinement of fire scenarios (including the consideration of fire growth and suppression), the determination of the fire damage and plant response, and the quantification of the fire scenarios including the assignment to specific plant damage states. The hazard occurrence frequency and a set of "worst-case" plant impacts are assessed for each scenario developed in the spatial interactions analysis. Each scenario is then screened quantitatively to determine its risk significance in relation to other initiating events. Scenarios that are found to be quantitatively insignificant are documented and removed from further consideration. For those scenarios that are retained, additional analysis is performed to systematically refine the initiating event frequency and functional impacts and to develop a more realistic assessment of the risk significance of each retained scenario. Section 4 of Bohn and Lambright (1990) provides a more detailed discussion of the analysis of fire-induced scenarios, once the fire scenarios have been identified. The goals for this task are accomplished by the performance of five activities:

1. Assessment of the fire hazard occurrence frequencies
2. Assessment of worst-case plant impact for each scenario
3. Performance of quantitative scenario screening
4. Refinement of scenario frequency and impact analysis
5. Retention of risk significant scenarios.

Each of these activities is discussed below.

12.2.1 Activity 1 — Assessment of the Fire Hazard Occurrence Frequencies

Each fire scenario in the spatial interactions analysis is defined at the location level, i.e., a scenario describes a fire of any severity that can occur anywhere in a given location. The objective of the scenario frequency assessment is to quantify consistently a plant-specific fire hazard occurrence rate for each of these locations.

A quantitative screening process is performed during the detailed scenario analysis phase of the analysis. The screening process applies numerical criteria to determine the relative risk significance of each fire scenario. If it is determined that a scenario is insignificant compared with these numerical screening criteria, that scenario is removed from further consideration in the PRA models. Therefore, it is very important that the fire occurrence frequencies assessed during this activity of the process satisfy the following objectives:

- The frequency of the postulated scenario must consistently account for industry fire data and any plant-specific experience for the type of hazard being evaluated in the type of location being modeled.

- The frequency of the postulated scenario must provide a conservative upper bound for the actual frequency of more detailed event scenarios that may eventually be developed for the location. In other words, the total scenario frequency may be consistently subdivided to more realistically represent any specific event scenario in the location, if it is necessary to develop more detailed models for the location.

These two objectives are somewhat counteractive. The first objective is to develop an event frequency that is as realistic as possible while the second objective is to develop an event frequency that is sufficiently conservative to ensure that the hazard scenario is not inappropriately screened from the PRA models. Thus, in effect, the analysis must develop an

initial frequency estimate that is "reasonably conservative" for each defined scenario.

The first activity of the fire frequency assessment involves a thorough review of the industry experience data to develop a "specialized generic database." This database should account for design features of the plant being evaluated and should be consistent with the scope of the PRA model and with the characteristics of the specific hazard scenarios defined for the analysis. If data from plants other than VVERs are used, care must be taken to properly interpret the data. Fire incidents that have occurred at a given location in a particular plant may be applicable for enhancing the fire-incident database for a different location in the Kalinin Nuclear Power Station. The experience data must also be screened to remove fire events that occurred during periods other than plant operation, such as during construction or refueling (since the Kalinin PRA only considers the risk of power operation).

The product from this activity of the frequency assessment process is the specialized generic database. This database should contain only the hazard event summaries considered relevant for the plant being modeled, for the specific operating conditions being evaluated, and for the specific scope of the functional impact locations and scenarios defined in the analysis. This database should be documented and should provide the generic industry experience input to the environmental hazard frequency analysis.

The industry event data can be combined with actual plant-specific experience through a two-stage Bayesian analysis that forms the basis for the fire hazard frequency assessment. This process is consistent with the evaluation of all other data in the PRA, including the frequencies for internal initiating events, component failure rates, component maintenance unavailabilities, and equipment common-cause failures.

Bayesian analysis allows the industry data to be combined with actual experience from the plant being studied. The first stage of this analysis develops a generic frequency distribution for each hazard that consistently accounts for the observed site-to-site variability in the industry experience data. The second stage updates this generic frequency to account specifically for the actual historical experience at Kalinin.

Estimates are made of the fraction of each hazard and hazard type for each location. For example, it would be noted that two of the six batteries at the plant are found in a specific location. The determination of the fraction of cables found in a specific location would also be made by a structured estimation process. These estimates are necessary in order to partition the hazard occurrence frequencies to specific locations.

In most cases, it is necessary to combine data for various types of hazards to develop the best possible frequency estimate for a particular location. This type of "composite" frequency analysis is best illustrated by an example. For example, an air compressor may be located in an open corner of a large cable spreading room. The air compressor may not be important for the PRA models. However, the spatial interactions analysts defined the functional impact location to include the entire cable spreading room. The estimated frequency for fire events in this location must account for the composite nature of the fire hazards. It is unreasonable to develop a fire occurrence frequency based only on "cable spreading room" fire events, even though the PRA impacts are derived only from failures of the cables. Use of only cable spreading room fire data would underestimate the expected frequency of fires in this location. On the other hand, it is also unreasonable to develop a fire occurrence frequency that is based on data from plant locations that typically contain air compressors, e.g., open areas of a turbine building. Direct use of only these data could significantly overestimate the expected frequency of fires in the cable spreading room because of lower traffic densities, less transient combustibles, etc. in these rooms as compared to in the turbine building.

These situations are addressed by developing a composite hazard frequency that accounts for the types of equipment and the relative density of equipment in each location. Continuing with the above example, a composite fire frequency would be developed for the cable spreading room by adding a fraction of the "turbine building air compressor" fire event frequency data to the cable spreading room fire event frequency data. The fractions are generally based on the equipment location information documented in the spatial interactions analysis. They are also often based on general observations from the plant walkdown and the personal experience and

judgment of the fire analysis experts. The fractions are not usually derived from detailed deterministic models or numerical analyses. The primary objective of this process is to develop a reasonable estimate for the hazard frequency that consistently accounts for the actual configuration of equipment in the location. Thus, for the cable spreading room example, it is not reasonable to assess a fire event frequency that is only based on either extreme of the available data. It seems reasonable to acknowledge that the air compressor may contribute to the frequency of fires in the room. The precise fraction used in the frequency calculation may be based only on the analyst's judgment. However, once the fraction is documented, it is possible to test whether the results are sensitive to that judgment by simply varying the numerical value within reasonable bounds.

12.2.2 Activity 2 — Assessment of Worst-Case Plant Impact for Each Scenario

The task Spatial Interactions identifies the PRA-related equipment that may be damaged by each hazard in a particular functional impact location. In this activity, analysts who are very familiar with the PRA event sequence models and system fault trees develop a conservatively bounding set of impacts for each hazard scenario. These impacts determine the specific equipment failure modes assigned when the hazard scenario is evaluated in the PRA risk models.

The initial impacts assigned during this phase of the analysis are considered to be the worst-case combination of failures that could conceivably be caused by the hazard. It is important to ensure that the assigned impacts provide a conservative upper bound for all actual failures that may occur during any fire scenario postulated to occur in the location. If it is determined that the scenario is quantitatively insignificant even within the context of these bounding impacts, then there is reasonable assurance that a more realistic appraisal of the potential impact would confirm the risk to be much lower than the screening value. The following examples illustrate the types of considerations used for assigning worst-case impacts.

At this point in the analysis, all equipment in the location is assumed damaged by the fire, regardless of the size of the location, the number of affected components, and the observed distribution of hazard severities. For most plant locations, the numerical risk contributions may be several times higher than from a more detailed hazards analysis because the occurrence frequency is usually dominated by relatively insignificant events, e.g., small fires of short duration and not by a fire that could presumably damage all equipment in a given location. This approach ensures that a conservative upper bound is generated for the risk contribution from any fire hazard event that may damage multiple components within the location. For example, it is not necessary to determine which specific cables may be damaged in a particular set of cable trays if the impact assessment assumes that **any** fire in the location damages **all** cables.

The assumed failure modes depend on the normal status of the equipment, the PRA model success criteria, characteristics of the location, and the type of vulnerability. For example, an electrical cable may not be vulnerable to a flooding event at a given location even if it were submerged by the flooding incident but is susceptible to potential damage had a fire occurred in that location.

All fires that affect electrical cables are assumed to eventually cause an open circuit in the cables. However, "hot shorts" may occur when insulation fails between adjacent conductors or between energized conductors and ground. These short circuits are only of concern in those portions of instrumentation and control circuits that produce signals to operate equipment. For example, a hot short in a power cable cannot start a motor. Therefore, hot shorts in power cables are modeled with the same impacts as open circuits; it is assumed that the affected motor will not operate. However, a hot short in a control circuit may cause a spurious signal to start the motor, if power is available to it. The impacts from possible hot shorts in control circuits are assessed by first assuming that power is available to operate the component when the short circuit occurs and then assuming that the power fails. For example, it is assumed that a hot short will cause a spurious signal to open a normally closed motor-operated valve. It is further assumed that power is available to the valve motor, that the

valve opens successfully, and that power is then lost to the valve motor. Thus, the net effect from this assessment is to leave the valve failed in the open position. This assessment of hot shorts is applied only for equipment failure modes that have a negative impact on the availability of PRA equipment. The models do not include credit for possible hot shorts that may reposition components in their required configuration for accident mitigation.

The same types of assumptions are applied to solid-state electronic circuits. It is first assumed that spurious control signals will reposition equipment in a state that has the worst possible impact on PRA system availability. After the equipment has changed state, it is then assumed that subsequent open circuits will prevent automatic or manual signals from restoring the components to the desired state.

The impact assessments do not account for the relative timing of possible failures or for design features that may prevent certain combinations of failures. For example, the PRA success criteria may require that a pump must be tripped to avoid possible damage after loss of oil cooling. A possible fire scenario may affect control circuits that signal cooling water supply valves, electronic circuits that process the automatic signals to trip the pump, and circuit breaker controls for the electrical bus that supplies power to the pump motor. The worst-case impacts from this scenario are bounded by the following combination of conditions:

- It is assumed that the cooling water supply is disabled by hot shorts and/or open circuits that affect the valve controls. This condition requires that the pump must trip.
- It is assumed that the pump trip circuits are disabled by hot shorts or open circuits that affect the electronic circuits.
- It is assumed that power remains available for the pump motor until the pump is damaged. If the affected bus also supplies power to other PRA equipment that must operate to mitigate the event, it is assumed that power is not available for these components as well.

This assessment provides the most conservative combination of impacts that could possibly occur, without regard to the relative timing of failures or the actual likelihood for any of the specific impacts.

The impact assessments at this stage of the analysis does not account for possible operator actions to override or bypass faulty control circuits or to operate equipment locally. No recovery actions are modeled for any damage caused directly by the fire hazard event. Other operator actions are modeled only within the context of the entire sequence of events initiated by the hazard scenario, consistently with dynamic actions evaluated for similar internal initiating events.

The affected PRA equipment and the functional impacts from each hazard scenario are listed in each scenario table as shown in Section 8.3 (refer to data entry 7 in Table 8-3 as an example). In most cases, explanatory notes are also provided in data entry 9 to document more completely the bases for the assigned impacts.

If a particular hazard scenario requires more detailed analysis after the initial screening, this activity is the starting point for refinement of the scenario and a more realistic assessment of its impacts. The refinement process may involve several iterations. Each iteration typically includes a critical reexamination of only the most important impacts for that scenario. Conservatively, bounding assumptions are retained for impacts that have a relatively insignificant effect on overall risk. The goals of this process are to successively relax the most significant worst-case assumptions for each scenario, while retaining an overall conservative approach throughout the screening process.

12.2.3 Activity 3 — Performance of Quantitative Scenario Screening

Each hazard scenario is characterized by a hazard occurrence frequency and a set of functional impacts that affect the availability of various PRA components and systems. In this activity of the analysis, each scenario is propagated through the PRA risk models to determine a quantitative upper bound for its total contribution to plant risk. Thus, for example,

scenario FIRES1 from Table 8-4 is evaluated with an initiating event frequency of approximately 3.96×10^{-3} fire per room-year. The general transient event trees in that study were quantified for this event, assuming that all equipment modeled by Top Events BA, BU, and EP are failed. All other PRA equipment not affected directly by this fire are allowed to function at performance levels consistent with the availabilities evaluated in the respective system analyses. In the Kalinin PRA, it may be more appropriate to add house events to the system fault trees to represent the impact of specific environmental hazard-induced failures.

The plant damage state assignments will be consistent with those already developed for the internal events model, since the same plant event sequence logic models are employed to quantify the impact of the postulated fire hazard as were used for the internal event initiators.

Each hazard scenario generally results in a large number of individual detailed event sequences determined by the combined effects from the hazard-induced failures, the independent equipment successes and failures, and appropriate operator actions. All sequences that lead to core damage are recorded, and the total core damage frequency is compared with a numerical screening criterion to determine the relative risk significance of the scenario.

- If the total core damage frequency from all sequences initiated by the fire-initiated scenario falls below the screening criterion, it is concluded that the hazard produces an insignificant contribution to overall plant risk. The screening evaluation is documented, and the scenario is removed from further consideration in the PRA models.

- If the total core damage frequency from the fire-initiated scenario is higher than the screening criterion, the scenario is retained for further analysis in the PRA.

- If the potential plant damage state consequences from the fire-initiated scenario are unusual or severe, the scenario is retained for further analysis, even if its total core damage frequency is below the screening criterion.

Although the mechanics of this process are quite straightforward, several considerations must be noted to develop the proper perspective and context for this important activity in the overall analysis.

The methods used to assess the hazard initiating event frequency and the attendant impacts from the postulated scenario ensure that the evaluated core damage frequency is a conservative upper bound for the actual core damage frequency that may occur from any particular scenario in the location. The amount of conservatism depends on a variety of factors that cannot be estimated directly without considerable examination of the underlying models and analyses. However, the applied methods do provide assurances that no similar scenario can yield a higher core damage frequency evaluated during the screening analysis.

The applied screening criterion is an absolute numerical value that defines what is considered to be an "insignificant" core damage frequency. This type of analysis is not unique to the evaluation of internal plant hazards. In fact, implicit and explicit screening criteria are applied at all levels of a practical risk assessment. However, it is worth noting that the screening criterion for this analysis effectively defines an absolute lower limit for the resolution of concerns about the risk significance from internal plant hazards. Scenarios that fall below the limit are, by definition, considered to be insignificant. The relative importance of each scenario that remains above the limit is consistently evaluated with all other events modeled in the PRA.

Selection of the screening criterion is not a simple task. There are no general guidelines or "accepted" numerical values that can be broadly applied for any particular analysis. The selected value, however, must satisfy the following criteria:

- The value must be low enough to ensure that the screened scenarios are truly insignificant to the total risk from the plant being evaluated.

- The value must be high enough to facilitate a practical analysis that limits unreasonable efforts to develop detailed models for unimportant events.

- The value chosen should be relatively insensitive to future refinements in the PRA event sequence models, systems analyses, and data.

In general, these criteria are best served by delaying the screening process until the results from the analyses of internal initiating events have reached a point of relative maturity and stability, i.e., a point at which the internal events results are not expected to change "significantly." Screening values are typically selected to ensure that the total core damage frequency from each screened scenario is less than approximately 0.05 percent to 0.1 percent (i.e., 1/20 to 1/10 of 1 percent) of the total core damage frequency from all other contributors. Thus, for example, if the screening criterion is numerically equal to 0.1 percent of the total core damage frequency from all other causes, an absolute minimum of 1,000 screened hazard scenarios would be required to double the total core damage frequency. If the screening analysis is performed at an early stage of the PRA modeling process, it is then generally recommended that the screening values be set equal to a smaller percentage of the preliminary core damage frequency results. This avoids the need for inefficient rescreening if, and when, PRA modeling refinements have reduced the contributions from all other accident initiators.

Thus, the final screening value cannot be determined at this time. For some perspective, however, the screening value used in one recent study was 1×10^{-9} core damage event per year.

12.2.4 Activity 4 — Refinement of Scenario Frequency and Impact Analysis

Each fire hazard scenario that yields a total core damage frequency exceeding the screening criterion is retained for further analysis in the PRA models. The level of effort and the focus of these analyses are determined by a balanced examination of all the contributors to plant risk. In many cases, the upper-bound core damage frequency may be higher than the value used for screening the hazard, but the scenario remains a very small contribution to overall plant risk. Extensive effort to further refine these scenarios is not justified by practical considerations. Their conservatively bounding frequencies and impacts are simply retained in the PRA results.

An iterative process is performed to refine the models, if further analysis is warranted. This process involves careful reexamination of all assumptions and successive application of the previous analysis activities to develop systematically more realistic models for the scenario definition, the hazard frequency, and the assigned impacts. One or more of the following refinements are typically made during this phase of the analysis:

- The scenario may be subdivided into a set of constituent scenarios that are based on physical characteristics of the location and the hazard sources. This process allows the assignment of more realistic equipment impacts from each of the specific hazard conditions.

- The hazard may be subdivided into various severity levels that are based on observed experience from the generic and plant-specific databases. Each hazard severity level is examined to define a more realistic set of impacts that could be caused by an event with that severity.

- The assumed impacts from hot shorts and control circuit malfunctions may be reexamined to determine whether the assumed failure modes can actually occur in combination. Models may also be developed to probabilistically account for the relative timing of these failures.

- The event sequences initiated by the hazard may be refined to include possible operator recovery actions to mitigate the hazard or its impacts before specific event sequences progress to core damage.

- Models may be developed to more realistically account for phenomenological processes that occur during the stages of fire initiation, growth, detection, and mitigation.

The refinements that are applied for the reevaluation of a particular scenario depend on specific characteristics of the fire hazard, the location, and the functional impacts from the original analysis. The results from the screening evaluations often provide valuable insights into

the sensitivities of the most important assumptions and conservatisms. The refinement process for a particular scenario may involve several iterations. Each iteration typically includes a critical reexamination of only the most important impacts for that scenario. Conservatively bounding assumptions are retained for all impacts that remain relatively insignificant to overall risk. The goals of this process are to systematically relax the most significant worst-case assumptions for each scenario, while retaining an overall conservative approach throughout successive screening evaluations.

Whenever a hazard scenario is subdivided, a separate summary table is developed to document each refined scenario. These tables have the same format as the original scenario tables. They list the frequency for each refined hazard event and the specific impacts assigned to that event. The tables also document all deterministic and probabilistic analyses performed to develop the scenario frequency and its impacts. Each refined scenario is reevaluated in the PRA event and fault trees, and the results are reexamined in relation to the quantitative screening criteria.

Scenario refinement can continue further. Analyses may be required to refine how such phenomena as fire growth, detection, and suppression are addressed in specific scenarios. If this is the case, codes, such as COMPBRN IIIE (Ho, 1991), are available and have been used to support the probabilistic evaluation of specific fire scenarios. In practice, such codes are typically only used for a small number of scenarios. In fact, many PRAs do not carry the scenario refinement process to the point where such codes as COMPBRN are used.

12.2.5 Activity 5 — Retention of Risk Significant Scenarios

A combination of technical and practical considerations determine the final set of plant internal fire scenarios retained for quantification in the PRA results. All scenarios that exceed the quantitative screening criteria are retained in the PRA models. However, among these scenarios, the degree of refinement may vary considerably.

- The worst-case core damage frequency estimate for an initial hazard scenario may in some cases be numerically higher than the screening value, but the scenario still yields a very small contribution to overall plant risk. Extensive effort to further refine these scenarios is not justified by practical considerations, and they are simply retained in the PRA results with their conservatively bounding frequencies and impacts.

- In other cases, a scenario may be retained only after considerable additional analyses have been performed to refine conservative assumptions about its frequency and impacts.

Because of these differences, it is not possible to develop meaningful numerical estimates for the amount of conservatism that may remain in any particular scenario. However, it is generally true that scenarios that have been subject to reexamination and refinement should include less inherent conservatism than scenarios retained from an early stage of their definition.

It is also obviously not possible to develop any meaningful numerical estimates for the "actual" core damage frequency associated with the screened scenarios. The analysis process is structured to ensure that this frequency is very small, compared with other contributors to plant risk, but the value is certainly not zero. In support of the analysis conclusions, it is only possible to examine a worst-case conservative upper-bound numerical value that may be derived from the successive screening evaluations. This value is certainly not a realistic estimate of the actual core damage frequency from these scenarios. However, it can be stated with assurance that the "true" core damage frequency must be considerably lower than this composite screening value.

12.2.6 Additional Guidance

The approach outlined in this procedure guide is structured to produce a systematic, top-down, iterative, quantitative estimate of the risk from fires in nuclear power plants. A parallel and very similar approach is adopted to determine the risk associated with internal flooding. Both analyses

rely on the results of a structured spatial interactions analysis, however, each having different nuances.

In fires, significant damage, especially to electronic equipment, may be caused by smoke. The construction of postulated scenarios should consider the impact of smoke as well as potential negative impacts of fire mitigation systems. Operation of mitigation systems could affect the performance of operating equipment and could hinder or delay operators from entering specific areas for conducting emergency procedures. The effectiveness of fire detection and mitigation equipment are important factors when describing a fire scenario (starting with fire initiation and proceeding to growth, propagation, detection, and mitigation).

Also, some fire-incident databases already have a measure of detection and mitigation included in them. Specifically, some databases would not include a fire that is immediately detected and extinguished. Only fires that are "significant" are in such databases (i.e., some measure of mitigation is implicitly included in the data). Therefore, it is important to understand the nature of the data used before credit for detection and mitigation is claimed in the refinement of scenarios. It may prove easier to refine the frequency or impact of a particular scenario, and thus allow screening of the scenario, rather than to claim explicitly consider mitigation.

Fire frequencies are derived for a generic nuclear power plant based on fire sources. For example, a frequency is determined for "cable fires" at a nuclear power plant similar to the one under consideration using industry data. Although "generic" in nature, the data is specialized and screened to closely match the characteristics of the specific plant under consideration.

The generic fire hazard frequencies should be updated with the actual experiences at Kalinin.

The location of the specific hazards has been determined in the task Spatial Interactions. Estimates are required in this task for the fractions of each hazard source (e.g., cables, motor control centers, and logic cabinets) found in each location.

For a specific location, the frequency of occurrence of a fire of any size is determined by summing the fractional contribution of occurrence from each hazard found in that location.

A quantitative screening value is developed to identify those scenarios that will be carried forward in the analysis. In other words, only those scenarios that contribute appreciably to the frequency of core damage (or to specific undesirable plant damage states) are retained for further analysis.

Scenarios that survive the quantitative screening are refined, as appropriate. Refinement may involve such considerations as the extent of the damage initially postulated. The process proceeds iteratively until the scenarios that remain appropriately represent the risk associated with fires while containing acceptable conservatisms.

12.3 Products

During the performance of this task, the scenario tables that were initiated in the task Spatial Interactions are expanded upon and refined (an example of such a table is provided in Appendix I). The completed and refined scenario tables make up a key product for this effort.

As identified in the procedure guide for the task Documentation, the current task will produce draft material for the final report. Specifically, a draft portion of the "Fire Analysis" appendix of the main report will be produced. That draft section will include a description of the methodology and the analyses utilized to achieve the task objectives.

12.4 References

Bohn, M. P., and J. A. Lambright, "Procedures for the External Event Core Damage Frequency for NUREG-1150," NUREG/CR-4840, Sandia National Laboratories, November 1990.

Ho, V. S., et al., "COMPBRN IIIE: An Interactive Computer Code for Fire Risk Analysis," UCLA-ENG-9016, EPRI-NP-7282, Electric Power Research Institute, May 1991.

NRC, "The Use of PRA in Risk-Informed Applications," NUREG-1602, Draft Report for Comment, June 1997.

13. FLOOD ANALYSIS

The analytical tasks associated with a Level 1 probabilistic risk assessment (PRA) for accidents initiated by events internal to the plant (such as transients and loss-of-coolant accidents) are described in previous chapters. Other events both internal and external to the plant can cause unique initiating events or influence the way in which a plant responds to an accident. Figure 1.4 in Chapter 1 identifies three types of events (i.e., internal fires, internal floods, and seismic events) that require manipulation of the Level 1 internal event PRA in order to adequately model the plant response.

In this chapter, the way in which a Level 1 PRA is modified in order to model accidents initiated by internal floods is described. Figure 13.1 shows the important relationships between this task and the other major tasks of the PRA. These relationships are discussed below in Section 13.1.

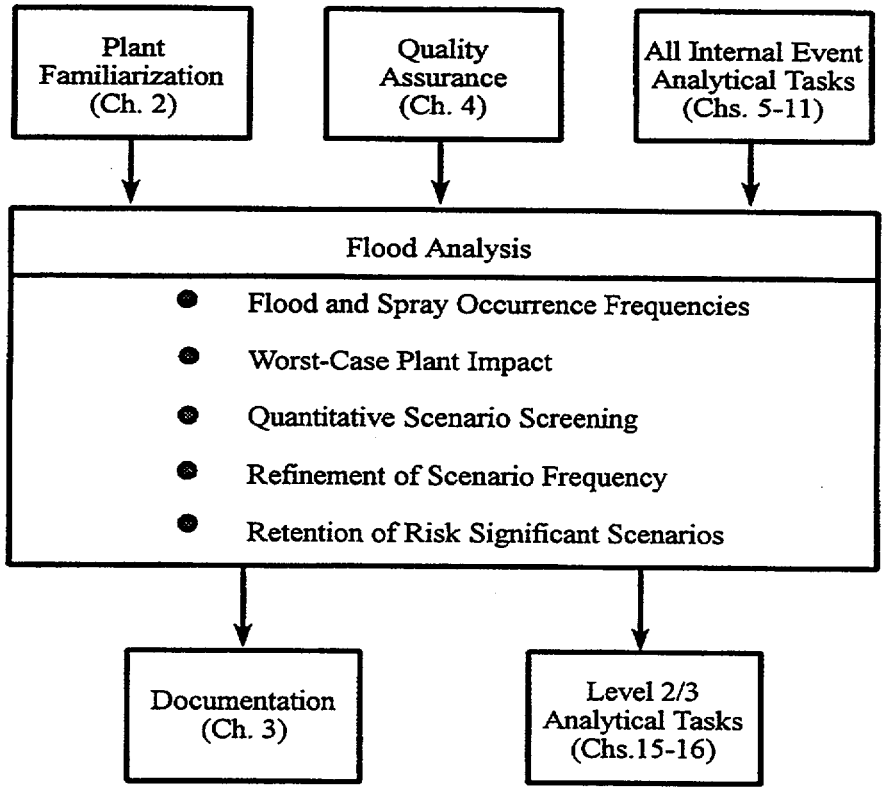


Figure 13.1 Relationships between flood analysis and other tasks

13.1 Relation to Other Tasks

As indicated in Figure 13.1, the Flood Analysis task has extensive interactions with all other PRA tasks:

Quality Assurance and Documentation. The Flood Analysis task has obvious interfaces with QA requirements and provides input to the PRA documentation.

All Internal Event Analytical Tasks. The current task utilizes the same overall analysis approach and procedures developed for the internal event PRA. In particular, this task builds on the information developed in the task Spatial Interactions (Section 8.3). The conduct of this task will require input from the tasks on Initiating Event Analysis (Chapter 6), Frequency of Initiating Events (Section 9.1), Event Sequence Modeling (Section 7.3), and System Modeling (Section 8.1). As scenarios are being developed to address floods, it is likely that specific operator

actions will be identified, thus requiring an interface with the task Human Reliability Analysis (Chapter 10).

Level 2/3 Analyses. Output from the Flood Analysis task provides information on accident sequence definition and on frequency of occurrence directly to the Level 2 task (refer to Chapter 15) which in turn provides source term information to the consequence and risk integration task (refer to Chapter 16). Whether or not Level 2/3 analyses are performed depends on the scope of the PRA (refer to Chapter 5).

13.2 Task Activities

While the internal flooding analysis of a PRA uses much the same processes and has the same attributes of a traditional full power internal events PRA (Chapters 6-11), the internal flooding analysis requires a significant amount of work to define and screen the most important flood sources and possible scenarios for further evaluation. These differences are described below in general terms. More detailed guidance can be found in NRC (1997) and Bohn (1990).

When preparing this chapter, some assumptions and limitations were made as indicated below:

- It is assumed that flood and spray incidence data from VVERs are available. The flood and spray incidence data should be of sufficient resolution to allow characterization according to the source of the flood or spray (e.g., piping failure, tank failure, etc.) and any other characteristics of the postulated event (e.g., maintenance error, passive failure, dynamic failure, etc.).

- It is assumed that a reasonable and practical quantitative screening criterion for culling out risk-insignificant events can be developed that would facilitate the completion of this task.

- The guidelines presented closely parallel those given in the procedure guide for the task Fire Analysis because of the similarity in the basic activities involved. However, since different analysts typically undertake the consideration of fire and flood analyses, individual procedure guides have been developed for each activity. Also, detailed phenomenological analyses are typically of secondary importance in conducting investigations of the impact of internal hazards in support of a PRA. Such investigations have the characteristic approach that can be described as an "iterative conservative screening" of scenarios.

- Care should be taken to include in the analysis those scenarios initiated by a non-flood incident (such as a pipe break) that might involve the introduction of water or steam into areas that include equipment of interest in the PRA. This requires the analyst to work closely with those who are developing the event sequence models to assure that all such events are accounted for in the model. Normally, the impact of flood water, spray, or steam resulting directly from a pipe break is already considered in the event sequence model if the failure results in a reactor or turbine trip.

- Analyses for other internal hazards (other than fire or flood) identified in the task Spatial Interactions should be carried out as part of this task using the guidelines presented here. Such hazards could include the dropping of heavy objects or. the spillage or leakage of caustic material.

The specific goals of this task include the development of a flood frequency database, the determination of the frequency of specific flood scenarios, the further development and refinement of flood scenarios, the determination of the flood damage to equipment and of the plant response, and the quantification of the flood-induced scenarios including the assignment to specific plant damage states. The hazard occurrence frequency and a set of "worst-case" plant impacts are assessed for each scenario developed in the spatial interactions analysis.

Each scenario is then screened quantitatively to determine its risk significance in relation to other initiating events. Scenarios that are quantitatively insignificant are documented and removed from further consideration. If a scenario remains quantitatively significant compared with the

screening criteria, it is retained for further evaluation. Additional analyses are then performed to systematically refine the hazard initiating event frequency and its functional impacts and to develop a more realistic assessment of its risk significance. During this process, the original flood or spray scenario is often subdivided into more detailed scenarios to more specifically account for actual impacts that can occur within the hazard location. Screening is, therefore, performed at various stages of the scenario-refinement process until final quantification of the PRA event sequence models. The goals for this task are accomplished by the performance of five activities:

1. Assessment of the flood and spray occurrence frequencies,
2. Assessment of worst-case plant impact,
3. Performance of quantitative scenario screening,
4. Refinement of scenario frequency and impact analysis,
5. Retention of risk significant scenarios.

Each of these activities is discussed below which makes use of the information found in Bohn (1990).

13.2.1 Activity 1 — Assessment of Flood and Spray Occurrence Frequencies

The objective of the scenario frequency assessment is to consistently quantify a plant-specific hazard occurrence rate for each location identified in the task Spatial Interactions as being vulnerable to the impacts of internal floods or spray.

Since a quantitative screening process is to be performed during the detailed scenario analysis phase of the internal plant hazards analysis, it is, therefore, very important that the hazard occurrence frequencies assessed during this activity of the process satisfy the following objectives:

- The hazard scenario frequency must consistently account for industry flood and spray data and any plant-specific experience that had occurred in the type of location being modeled.
- The hazard scenario frequency must provide a conservative upper bound in case more detailed event scenarios need to be developed for the location. In these cases, the total scenario frequency may be consistently subdivided to more realistically represent any specific event scenario in the location. Having a conservative upper-bound frequency for the gross scenario implies that the frequency of these more subtle, refined scenarios are captured, even after screening.

These objectives are somewhat counteractive. The first goal is to develop an event frequency that is as realistic as possible for a plant-specific risk assessment. The second goal is to develop an event frequency that is sufficiently conservative to ensure that the hazard scenario is not inappropriately screened from the PRA models. Thus, in effect, the analysis must develop an initial frequency estimate that is "reasonably conservative" for each defined scenario.

This first activity involves a thorough review of the industry experience data to develop a "specialized generic database." This database should account for design features of the plant, the scope of the PRA models, and the characteristics of the specific hazard. Each event in the industry-experience database should be reviewed to determine its applicability and to categorize the event with respect to the types of hazard scenarios defined. As for fire incidence data, if data from plants other than VVERs are used, care must be taken to interpret the data properly.

The resulting database should contain summaries of only those events that are relevant for the plant being modeled, for the specific operating conditions being evaluated, and for the specific scope of the functional impact locations and hazard scenarios defined in the analysis. This database should be documented and should provide the generic industry experience input to the hazard frequency analysis.

A two-stage Bayesian analysis combines the industry data with actual experience from the plant. The first stage of the Bayesian analysis develops a generic frequency distribution for each

hazard that consistently accounts for the observed site-to-site variability in the industry experience data. The second stage updates this generic frequency to account specifically for the actual historical experience at Kalinin.

Estimates are made of the fraction of each hazard and hazard type for each location. These estimates are necessary in order to partition the hazard occurrence frequencies to specific locations. In most cases, it is necessary to combine data for various types of hazards to develop the best possible frequency estimate for a particular location.

This process is consistent with the evaluation of all other data in the PRA, including the frequencies for internal initiating events, component failure rates, component maintenance unavailabilities, and equipment common-cause failures.

13.2.2 Activity 2 — Assessment of Worst-Case Plant Impact for Each Scenario

In the task Spatial Interactions, PRA-related equipment that may be damaged by each hazard in a particular functional impact location was identified. In this activity, analysts who are very familiar with the PRA event sequence models and system fault trees develop a conservatively bounding set of impacts for each hazard scenario. These impacts determine the specific equipment failure modes assigned when the hazard scenario is evaluated in the PRA risk models.

The initial assessment of these impacts are considered to be the worst-case combination of failures that could reasonably be caused by the hazard. It is important to ensure that the assigned impacts provide a conservative upper bound for all actual failures that may occur during any flood or spray scenario in the location. If it is determined that the scenario is quantitatively insignificant with these bounding impacts, then there is assurance that a more realistic evaluation would confirm that the attendant risk would also be much lower than the screening value.

At this point in the analysis, it is conservatively assumed that all equipment in the location is damaged by the hazard (either by submergence or spray), regardless of the size of the location, the number of affected components, and the observed distribution of hazard severities. The assumed failure mode for flood or spray events is usually "loss of function" of the susceptible equipment. For most locations, this assessment provides numerical risk contributions that may be several times higher than those that would be evaluated through a more detailed analysis. This is because the occurrence frequency for most hazards is dominated by relatively insignificant events, e.g., relatively small leakage events. However, the impacts are postulated to be the result of an extremely large flood or spray event, which is a highly unlikely, low frequency event. This approach ensures that a conservative upper bound is evaluated for the risk contribution from any hazard event that may damage multiple components within the location. That is, an event frequency of more frequent, insignificant events is linked to postulated impacts that may be attributable to a less frequent, more catastrophic scenario.

The impact assessments do not account for the relative timing of possible failures or for design features that may prevent certain combinations of failures. For example, the PRA success criteria may require that a pump must be tripped to avoid possible damage after loss of oil cooling. A possible flood scenario may affect a control panel for the cooling water supply pump. The worst-case impacts from this scenario are bounded by the following combination of conditions:

- It is assumed that the cooling water supply is disabled by the flood event. This condition requires that the pump must trip.
- It is assumed that the pump trip circuits are disabled by the flood or spray event if these circuits are located in the same susceptible cabinet.
- It is assumed that power remains available for the pump motor until the pump is damaged because of lack of cooling.

The impact assessments do not account for possible operator actions to override or bypass faulty control circuits or to operate equipment locally. No recovery actions are modeled for any

damage caused directly by the hazard event. Other operator actions are modeled only within the context of the entire sequence of events initiated by the hazard scenario, consistently with dynamic actions evaluated for similar internal initiating events.

Accordingly, the most conservative combination of impacts that could possibly occur, without regard to the relative timing of failures or the actual likelihood for any of the specific impacts, are used in this assessment.

As this activity proceeds, the affected PRA equipment and the functional impacts from each hazard scenario are listed in data entry 7 of each scenario table as shown in Section 8.3. In most cases, explanatory notes are provided also in data entry 9 to more completely document the bases for the assigned impacts.

If a particular hazard scenario requires more detailed analysis, this activity is the starting point since the refinement process may involve several iterations. Each iteration typically includes a critical reexamination of only the most important impacts to plant equipment for that scenario. Conservatively bounding assumptions are retained for impacts that have a relatively insignificant effect on overall risk. The goals of this process are to successively relax the most significant worst-case assumptions for each scenario, while retaining an overall conservative approach throughout the screening process.

13.2.3 Activity 3 — Performance of of Quantitative Scenario Screening

Each flood or spray scenario is characterized by a hazard occurrence frequency and a set of functional impacts that affect the availability of various PRA components and systems. In this activity of the analysis, each scenario is propagated through the PRA risk models to determine a quantitative upper bound for its total contribution to plant risk. In the Kalinin PRA, it may be appropriate to add house events to the system fault trees to represent the impact of specific environmental hazard-induced failures.

Note that since the same plant event sequence logic models are used to quantify the impact of the postulated environmental hazards as were used for the internal event initiators, the plant damage state assignments are consistent with those already developed for the internal events model.

In general, each scenario results in a large number of individual detailed event sequences determined by the combined effects from failures induced by the internal flood scenario, independent equipment successes and failures, and appropriate operator actions. All sequences that lead to core damage are recorded, and the total core damage frequency is compared with a numerical screening criterion to determine the relative risk significance of the scenario.

- If the total core damage frequency from all sequences initiated by the scenario falls below the screening criterion, it is concluded that the hazard produces an insignificant contribution to overall plant risk. The screening evaluation is documented, and the scenario is removed from further consideration in the PRA models.

- If the total core damage frequency from the scenario is higher than the screening criterion, the scenario is retained for further analysis in the PRA.

- If the potential plant damage state consequences from the scenario are unusual or severe, the scenario is retained for further analysis, even if its total core damage frequency is below the screening criterion.

Although the mechanics of this process are quite straightforward, several considerations must be noted to develop the proper perspective and context for this critical activity in the analysis.

The methods used to assess the hazard initiating event frequency and the scenario impacts ensure that the evaluated core damage frequency is a conservative upper bound for the actual core damage frequency that may occur from any particular scenario in the location. The amount of conservatism depends on a variety of factors, which cannot be estimated directly without considerable examination of the underlying models and analyses. However, the applied methods provide assurance that the conditional

core damage resulting from this scenario will not occur at a higher frequency.

This screening approach is not unique to the evaluation of internal plant hazards. Implicit and explicit screening criteria are applied at all levels of a practical risk assessment. The issue of basic event truncation in previous tasks can be construed as some form of screening. It is worth noting that the screening criterion used in this task effectively defines an absolute lower limit for the resolution of concerns about the risk significance from internal plant hazards. Scenarios that fall below the limit are, by definition, considered to be insignificant, and the relative importance of each scenario that remains above the limit is evaluated consistently with all other events modeled in the PRA.

Selection of the numerical screening criterion is not a simple task. There are no general guidelines or "accepted" numerical values that can be broadly applied for any particular analysis. The selected value should be:

- low enough to ensure that the screened scenarios are truly insignificant to the total risk,
- high enough to facilitate a practical analysis and to limit efforts to develop detailed models for unimportant events, and
- relatively insensitive to any future refinements in the PRA event sequence models, system analyses, and data.

Based on the above, the screening process should begin when the results from the internal initiating events phase have reached a point of relative maturity and stability, i.e., a point at which the internal events results are not expected to change "significantly." Screening values are typically selected to ensure that the total core damage frequency from each screened scenario is less than approximately 0.05 percent to 0.1 percent (i.e., 1/20 to 1/10 of 1 percent) of the total core damage frequency from all other contributors. Thus, for example, if the screening criterion is numerically equal to 0.1 percent of the total core damage frequency from all other causes, an absolute minimum of 1,000 screened hazard scenarios would be needed to double the total core damage frequency. If the screening analysis is performed at an earlier stage of the PRA modeling process, it is generally recommended that the screening values be set at even a smaller percentage of the preliminary core damage frequency. This avoids the need for inefficient rescreening of the internal hazard scenarios after modeling refinements reduce the contributions from all other initiators.

The final screening value thus cannot be determined at this time. For perspective, however, the screening value used in one recent study was 1×10^{-9} core damage event per year.

13.2.4 Activity 4 — Refinement of Scenario Frequency and Impact Analysis

Each hazard scenario having a total core damage frequency that exceeds the screening criterion is retained for further analysis in the PRA models.

If further analysis is warranted, an iterative process is performed to refine the models. This process involves careful reexamination of all assumptions and successive application of the previous analysis activities to systematically develop more realistic models for the scenario definition, the hazard frequency, and the assigned impacts. One or more of the following refinements are typically made during this phase of the analysis:

- The scenario may be subdivided into a set of several constituent scenarios that are based on physical characteristics of the location and the hazard sources. This process allows the assignment of more realistic equipment impacts from each of the specific hazard conditions.
- The hazard may be subdivided into various severity levels that are based on observed experience from the generic and plant-specific databases. Each hazard severity level is examined to define a more realistic set of impacts that could be caused by an event with that severity.
- The assumed impacts from control circuit malfunctions may be reexamined to determine whether the assumed

failure modes can actually occur in combination. Models may also be developed to probabilistically account for the relative timing of these failures.

- The event sequences that are initiated by the hazard may be refined to include possible operator recovery actions that may be put into place to mitigate the hazard or its impacts before specific event sequences progress to core damage.

The refinements applied for a particular scenario depend on specific characteristics of the hazard, the location, and the functional impacts from the original analysis. The results from the screening evaluations often provide valuable insights about the most important assumptions and conservatisms that must be reexamined. The refinement process for a particular scenario may involve several iterations. Each iteration typically includes a critical reexamination of only the most important impacts for that scenario. Conservatively bounding assumptions are retained for all impacts that remain relatively insignificant to overall risk. The goals of this process are to systematically relax the most significant worst-case assumptions for each scenario, while retaining an overall conservative approach throughout successive screening evaluations.

Whenever a hazard scenario is subdivided, a separate summary table is developed to document each refined scenario. These tables have the same format as the original scenario tables. They list the frequency for each refined hazard event and the specific impacts assigned to that event. The tables also document all deterministic and probabilistic analyses performed to develop the scenario frequency and its impacts. Each refined scenario is reevaluated in the PRA event trees and fault trees, and the results are reexamined in relation to the quantitative screening criteria.

Scenario refinement can continue further if warranted. Analyses that consider leakage rates, drainage rates, component vulnerabilities, and potential mitigative actions, for example, can be used to support the removal of conservatisms in selected scenarios. It is expected that such analyses will be required only for a limited number of flood or spray scenarios.

13.2.5 Activity 5 — Retention of Risk-Significant Scenarios

A combination of technical and practical considerations determine the final set of scenarios retained for quantification in the PRA results. All scenarios that exceed the quantitative screening criteria are retained in the PRA models. However, the degree of refinement may vary considerably among these scenarios:

- In some cases, the worst-case core damage frequency estimate for an initial hazard scenario may be numerically higher than the screening value, but the scenario remains a very small contribution to overall plant risk. Extensive effort to further refine these scenarios is not justified by practical considerations, and they are simply retained in the PRA results with their conservatively bounding frequencies and impacts.

- In other cases, a scenario may be retained only after considerable additional analyses have been performed to refine conservative assumptions about its frequency and impacts, either by refining the scenarios or by using phenomenological modeling.

Because of these differences, it is not possible to develop meaningful estimates for the amount of conservatism that may remain in any particular scenario. However, the scenarios that have been reanalyzed should contain lesser conservatism than scenarios retained from an earlier stage of the analysis.

It is not possible to develop any meaningful numerical estimates for the "actual" core damage frequency associated with the screened scenarios. The analysis process is structured to ensure that this frequency is very small compared with other contributors to plant risk, but the value is certainly not zero. In support of the analysis conclusions, it is only possible to examine a conservative upper-bound numerical value that may be derived from the successive screening evaluations. This value is certainly neither a best

nor realistic estimate of the core damage frequency from these scenarios. However, the "true" core damage frequency must be considerably lower than this composite screening value.

13.2.6 Additional Guidance

The approach outlined in this procedure guide is structured to produce a systematic, top-down, iterative estimate of the risk due to postulated internal flood or spray events. A parallel and very similar approach is adopted to determine the risk associated with fires. Both analyses rely on the results of a structured spatial interactions analysis.

Specific scenarios that involve flooding or spraying of hot water or steam can degrade the ambient environment. However, not much information is available concerning the operation of equipment in high temperature or humid environments. In that case, it is usually assumed that the equipment would fail (fail to continue to run or fail to start for motors; fail to transfer for valves) if the environmental qualification envelope for the particular piece of equipment is exceeded. Consideration of the environmental impact on control circuitry (especially solid-state equipment) is more complex. Control failures and/or spurious signals can be postulated. The analysis should clearly specify what failure modes are modeled and should outline the rationale for choosing these failure modes.

The development of flood scenarios should include the consideration of propagation of the flood via doorways, drains, and ventilation ductwork. These pathways should have been considered in the information developed as part of the task Spatial Interactions. In addition, if the failure of barriers or structures due to static loading is credible and could lead to a more severe flood impact, failure of such barriers should also be considered.

Typically, no credit is taken for drains as a means of mitigating a flood unless it is found in subsequent iterations that the drains may be an important factor in the definition of the scenario. In that case, their performance should be investigated, at least probabilistically. In some plants, the flow characteristic of individual drains has not been demonstrated since start-up, in which case assurances must be given that construction material or other debris has not significantly altered the capabilities of the specific drains under consideration.

Flood frequencies are derived for a generic nuclear power plant based on potential flood sources. For example, a flood frequency may be determined for "heat exchangers" (due, for example, to errors during maintenance events) at a nuclear power plant similar to the one under consideration using industry data. Although "generic" in nature, the data is specialized and screened to match closely the characteristics of the specific plant under consideration. The generic flood hazard frequencies are to be updated with the actual experiences at Kalinin.

The location of the specific hazards has been determined in the task Spatial Interactions. Estimates are required in this task for the fractions of each flooding source (e.g., tanks or piping) found in each location.

For a specific location, the frequency of occurrence of a flood or spray of any size is determined by summing the fractional contribution of occurrence from each flood or spray hazard found in that location.

A quantitative screening value is developed to identify those scenarios that will be carried forward in the analysis. Only those scenarios that contribute appreciably to the frequency of core damage (or to specific undesirable plant damage states) are retained for further analysis and/or refinement.

Refinement may involve such considerations as the extent of the damage initially postulated. The process proceeds until the scenarios that remain appropriately represent the risk associated with internal floods while containing acceptable conservatisms.

13.3 Products

During the conduct of this task, the scenario tables initiated in the task Spatial Interactions are expanded upon and refined (an example of such a table is provided in Appendix J). The completed and refined scenario tables make up a key product for this effort.

As identified in the task Documentation, the current task will produce draft material for the final report. Specifically, a draft portion of the "Flood Analysis" appendix of the main report will be produced. That draft section will include a description of the methodology and the data analyses utilized to achieve the task objectives.

13.4 References

Bohn, M. P., and J. A. Lambright, "Procedures for the External Event Core Damage Frequency for NUREG-1150," NUREG/CR-4840, Sandia National Laboratories, November 1990.

NRC, "The Use of PRA in Risk-Informed Applications," NUREG-1602, Draft Report for Comment, June 1997.

14. SEISMIC ANALYSIS

The analytical tasks associated with a Level 1 probabilistic risk assessment (PRA) for accidents initiated by events internal to the plant (such as transients and loss-of-coolant accidents [LOCAs]) are described in Chapters 5 through 11. Other events both internal and external to the plant can cause unique initiating events or influence the way in which a plant responds to an accident. Figure 1.4 in Chapter 1 identifies three types of events (i.e., internal fires, internal floods, and seismic events) that require manipulation of the Level 1 internal event PRA in order to adequately model the plant response.

In this chapter, the way in which a Level 1 PRA is modified in order to model accidents initiated by earthquakes occurring at or near the plant site is described. This means that the frequency and severity of the ground motion must be coupled to models that address the capacity of plant structures and components to survive each possible earthquake. The effects of structural failure must be assessed, and all the resulting information about the likelihood of equipment failure must be evaluated using the Level 1 internal event probabilistic logic model of the plant. This procedure guide is largely based on several earlier guides and studies (Bohn and Lambright, 1990; IAEA, 1995; and PG&E, 1988). Material from these sources is used here without specific citations.

Figure 14.1 shows the important relationships between this task and the other major tasks of the PRA. These relationships are discussed below in Section 14.1.

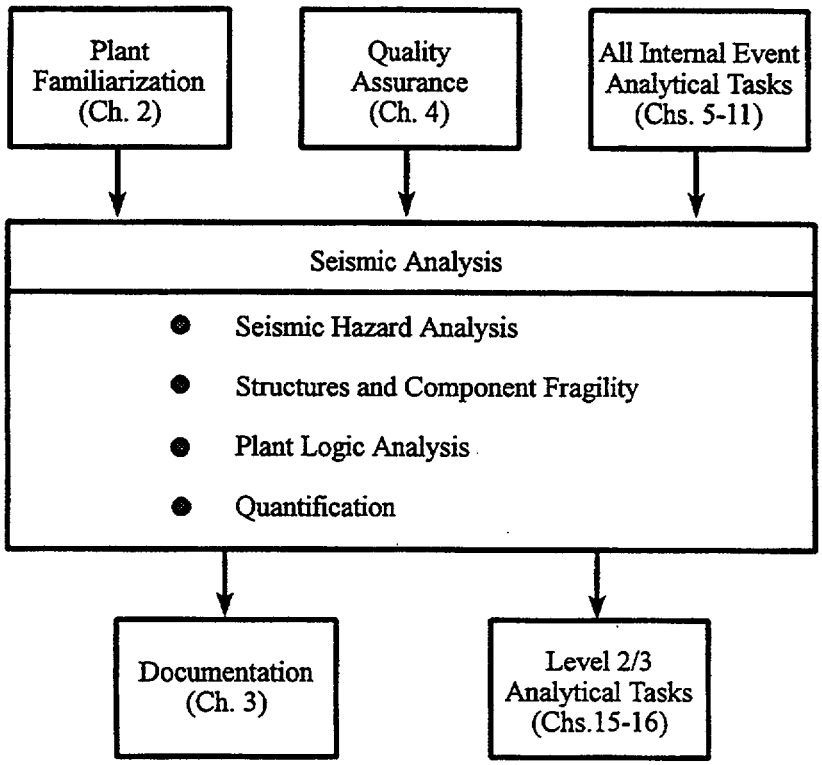


Figure 14.1 Relationships between seismic analysis and other tasks

14.1 Relation to Other Tasks

As indicated in Figure 14.1, the Seismic Analysis task has extensive interactions with all other PRA tasks:

Quality Assurance and Documentation. The Seismic Analysis task has obvious interfaces with QA requirements and provides input to the PRA documentation.

All Internal Event Analytical Tasks. The current task utilizes the same overall analysis approach and procedures developed for the internal event PRA. In particular, this task builds on the information developed in the task Spatial Interactions (Section 8.3). The conduct of this task will require input from the tasks dealing with Initiating Event Analysis (Chapter 6), Frequency of Initiating Events (Section 9.1), Event Sequence Modeling (Section 7.3), and System Modeling (Section 8.1). It is also likely that specific operator actions will be identified in the seismic scenarios, thus prompting an interface with the task Human Reliability Analysis (Chapter 10).

Level 2/3 Analyses. Output from the Seismic Analysis task provides information on accident sequence definition and on frequency of occurrence directly to the Level 2 task (refer to Chapter 15) which in turn provides source term information to the consequence and risk integration task (refer to Chapter 16). Whether or not Level 2/3 analyses are performed depends on the scope of the PRA (refer to Chapter 5).

14.2 Task Activities

A seismic PRA assumes that a single parameter (effective ground acceleration) characterization of the earthquake, when combined with treatments of uncertainty and dependency, can provide an adequate representation of the effects of seismic events on plant operations. This approach acknowledges that different earthquakes (in terms of energy, frequency spectra, duration, and ground displacement) can have the same effective acceleration. Therefore, there is not only randomness in the frequency of earthquakes but also large uncertainty in the specific characteristics of earthquakes of a given effective acceleration. These uncertainties have implications for modeling dependencies among failures of various equipment under excitation by earthquakes of a particular effective acceleration. Systems analysts and fragility experts must work closely together to determine how to model these dependencies.

A nuclear power plant is usually designed to ensure the survival of all buildings and emergency safety systems for a particular size earthquake, i.e., a design basis or a safe shutdown earthquake. The assumptions used in the design process are deterministic and are subject to considerable uncertainty. It is not possible, for example, to predict accurately the worst earthquake that will occur at a given site. Soil properties, mechanical properties of buildings, and damping in buildings and internal structures also vary significantly. To model and analyze the coupled phenomena that contribute to the frequency of radioactive release, it is, therefore, necessary to consider all significant sources of uncertainty as well as all significant interactions. Total risk is then obtained by considering the entire spectrum of possible earthquakes and integrating their calculated consequences. This point underscores an important requirement for a seismic PRA--that the nuclear power plant must be examined in its entirety, as a system.

During an earthquake, all parts of the plant are excited simultaneously. There may be significant correlation between component failures, and, hence, the redundancy of safety systems could be compromised. For example, in order to force emergency core cooling water into the reactor core following a pipe leak or break, certain valves must open. To ensure reliability, two valves are located in parallel so that should one valve fail to open, the second valve would provide the necessary flow path. Since valve failure due to random causes (corrosion, electrical defect, etc.) is an unlikely event, the provision of two valves provides a high degree of reliability. However, during an earthquake, both valves would experience the same accelerating forces, and the likelihood is high that both valves would be damaged, if one valve is damaged. Hence, the redundancy built into the design would be compromised. The potential impact from this "common-cause" failure possibility represents a potentially significant risk to safely shutting down nuclear power plants during an earthquake.

The scope of the seismic analysis should include:

- Seismic Hazard Analysis, i.e., the likelihood and magnitude of potential earthquakes (represented in terms of seismic hazard curves), including the transfer of energy from the fault source to the power plant site and the interaction between the soil underlying the power plant and the structural response,
- Structures and Component Fragility Analysis, i.e., the coupling of responses between buildings and the reactor vessels, piping systems, and emergency safety systems housed therein,
- Plant Logic Analysis, i.e., the development of the accident scenarios that vary according to the types of failures assumed to occur from the seismic event and the success or failure of the engineered safety features intended to mitigate the consequences of the accident,
- Quantification, i.e., convolution of the seismic hazard curves with the structure and component fragility curves to obtain the probability of failure of each element under discrete earthquake acceleration levels along with the integrated plant response and proper treatment of seismic coupling earthquake,
- Documentation.

Each of these activities is discussed below, and the products are summarized in Section 14.4. These tasks are linked in that the first two are used to formulate the required changes to the internal events plant model to support seismic PRA. Although the first three tasks will be performed by different groups, these groups must work in concert to ensure proper and consistent modeling of seismic-induced events.

Seismically induced failures can cause one or more of the internal event initiators already described in Chapter 6 to occur. Although specific seismic accelerations are generally considered to yield specific "initiating events," the results from such accelerations must interrupt full power operations in functional ways already described in previous tasks. The difference with seismic events, as compared to other upset conditions, is that multiple plant functional initiators may occur along with seismically induced failures of equipment needed for controlling the event sequence as well as physically and psychologically impacting operator performance.

14.2.1 Activity 1 — Seismic Hazard Analysis

For a given site, the hazard curve is derived from a combination of recorded earthquake data, estimated earthquake magnitudes of known events for which no data are available, review of local geological investigations, and use of expert judgment from seismologists and geologists familiar with the region. The region around the site (say within 100 km) is divided into zones, each zone having an (assumed) uniform mean rate of earthquake occurrence. This mean occurrence rate is determined from the historical record, as is the distribution of earthquake magnitudes. An attenuation law is determined that relates the ground acceleration at the site to the ground acceleration at the earthquake source, as a function of the earthquake magnitude. The uncertainty in the attenuation law is specified by the standard deviation of the data (from which the law was derived) about the mean attenuation curve. These four pieces of information (zonation, mean occurrence rate for each zone, magnitude distribution for each zone, and attenuation) are combined statistically to generate the hazard curve.

The low level of seismic activity and the lack of instrument recordings generally make it difficult to carry out a seismic hazard analysis using historic data alone. Current seismic risk method use the judgment of experts who are familiar with the area under consideration to augment the database.

Expert opinion is solicited on input parameters for both the earthquake occurrence model and the ground motion (attenuation) model. Questions directed to experts cover the following areas: (a) the configuration of seismic source zones, (b) the maximum magnitude or intensity earthquake expected in each zone, (c) the earthquake activity rate and occurrence statistics associated with

each zone, (d) the methods for predicting ground motion attenuation in the zones from an earthquake of a given size at a given distance, and (e) the potential for soil liquefaction.

Using the information provided by experts, seismic hazard evaluations for the site are performed. The hazard results thus obtained using each expert's input are combined into a single hazard estimate. Approaches used to generate the subjective input, to assure reliability by feedback loops and crosschecking, and to account for biases and modes of judgment are described in detail in Bernreuter (1981).

To perform the seismic PRA, a family of hazard curves and either ensembles of time histories or site ground motion spectra must be available. To obtain these for a site with no previous investigation usually involves 6 to 12 months of effort to develop and process a database on earthquake occurrences and attenuation relations as described above. For some locations (e.g., sites in the western United States, where the hazard curves are closely tied to local tectonic features that can be identified and for which a significant database of recorded earthquake time histories exists), it is usually necessary to go through this process for each individual plant site.

Evaluation of the site-specific hazard curve is generally performed by geologists and ground motion specialists using the methods described in Bernreuter (1981), IAEA (1993), and PG&E (1988).

14.2.2 Activity 2 — Structures and Component Fragility Analysis

Using the models developed for internal events PRA as a basis, a list of equipment and the buildings that house them must be provided to the fragility analysts. Necessarily, this list will combine similar equipment into convenient categories rather than identifying each of the possible risk-related components in the plant. Typically, equipment with median acceleration capacities of about 4g or higher will not be analyzed because the frequency of such events that can generate this acceleration on equipment is very low.

The fragility descriptions are based on a two-parameter lognormal distribution where β_R is the logarithmic standard deviation due to randomness in the earthquake and β_U is the logarithmic standard deviation due to uncertainty or state of knowledge (Kennedy et al., 1980; Kaplan, Perla, and Bley, 1983). A simplified composite or mean fragility curve (Kaplan, Bier, and Bley, 1992) can be defined with a single composite logarithmic standard deviation, β_U. The tails of these distributions are considered to be conservative. Therefore, the following is the basis for truncation of the fragility curves in this project:

1. The uncertainty variability, β_U, should not be truncated.

2. The random variability, β_R, should be truncated at about 1 percent failure fraction for relatively ductile component failure modes, such as in piping systems and in civil structures. In addition to the civil structures and piping, components in the plant that are generally in this category are:

   - reactor internals
   - pressurizer
   - reactor coolant pumps
   - control rod drives
   - component cooling water surge tank
   - battery racks
   - impulse lines
   - cable trays and supports
   - heating, ventilation, and air conditioning ducting and supports.

3. For all other plant components, the truncation point should be at a significantly lower failure fraction, 0.1 percent.

Since the response spectra from a given earthquake are common to all of the plant components to some degree, we can expect some correlation of failure between components having similar vibrational frequencies. Studies to assess these correlations (Kennedy et al., 1988) concluded the following:

- Except at high frequencies (greater than about 18 Hz), responses of identical components with the same frequencies should be treated as totally dependent, even when mounted at different elevations in different structures located at the site.

- Responses of components with different vibrational frequencies are essentially uncorrelated even when mounted on the same floor.

- Fragilities of components with different vibrational frequencies and adjacently mounted should be treated as independent.

- The piping fragility should be treated such that each segment, between rigid supports or between equipment, is considered to be independent of the other segments.

- The fragility of conduits and cable trays is considered to represent all the conduits and cable trays largely because of the natural flexibility existing in cables; that is, individual cable trays and conduits are not considered independently. By their very nature, large physical movements do not mean cable failure.

- The fragility of heating, ventilation, and air conditioning ducts is considered to represent that of all the ductwork supporting a single safety system.

Using these guidelines, the plant model assumes total dependency for identical equipment at the site (that is, if one fails, all of the same type fail). All other equipment situations follow the definitions above or otherwise are considered independent.

14.2.3 Activity 3 — Plant Logic Analysis

Seismic event trees should be derived from those already developed from the internal events analysis. However, passive components, such as pipe segments, tanks, and structures which were not modeled because of their low probability of failure, must now be included in the event tree analyses. Seismic failure of passive components is possible and must be investigated in the fragility analysis of Activity 2. Component failure due to seismic failure of structures housing (or supporting) the component must be considered as well. These new failure modes will entail revision of fault trees and event trees generated in the internal events analysis. One particular seismic-related failure mode is relay chatter (Bley et al., 1987; Budnitz, Lambert, and Hill, 1987; Lambert and Budnitz, 1989). Relays may chatter momentarily (electrical contacts open and close) causing lockup of control circuits that can only be overridden by completely deenergizing the control circuits, which can be a difficult situation for operators to diagnose. A comparable issue is fire-induced spurious signals that have to be addressed in a fire risk analysis.

Earthquakes can lead to seismically induced fires, which may be difficult to control due to the effect of the earthquake on plant accessibility and human performance. Similarly, seismically induced floods should be investigated. Just the impacts on accessibility and human performance can cause human failure events that would otherwise not occur under normal circumstances.

LOCAs (from vessel rupture, large, medium and small LOCAs) and transient events should be included in the seismic analysis. The two types of transients that should be considered are those in which the power conversion system is initially available and those in which the power conversion system is unavailable as a direct consequence of the initiating event.

The frequencies of vessel rupture (reactor pressure vessel) and large LOCA events can be determined from the probability of seismic failure of the major reactor coolant system component supports. The medium and small LOCA initiating event frequencies can be computed based on a statistical distribution of pipe failures computed as part of the Seismic Safety Margins Research Program (SSMRP).

The probability of transients with the power conversion system unavailable is based on the probability of loss-of-offsite power. This will always be the dominant cause of these transients

(for the majority of plants for which loss-of-offsite power causes loss of main feedwater). The probability of the transients with the power conversion system available is computed from the condition that the sum of all the initiating event probabilities considered must be unity. The hypothesis is that given an earthquake of reasonable size, at least one of the initiating events will occur.

The fault trees developed for the internal events analysis are used in this analysis although the fault trees will require modification to include basic events with seismic failure modes and resolving the trees for determining pertinent cutsets for seismic PRA calculations. A screening analysis is performed to identify the seismic cutsets. Conservative basic event probabilities, based on the seismic failure probabilities evaluated at a high earthquake peak ground acceleration level combined with the random failure probabilities, are used to probabilistically cull these trees that assures that important correlated cutsets are not lost (involving dependent seismic failure modes).

Component seismic fragilities are obtained either from a generic fragility database or developed on a plant-specific basis for components not fitting the generic component descriptions. At least two sources of fragility data are available. The first is a database of generic fragility functions for seismically induced failures originally developed as part of the SSMRP (Smith et al., 1981). Fragility functions for the generic categories were developed based on a combination of experimental data, design analysis reports, and an extensive expert opinion survey. The experimental data utilized in developing fragility curves were obtained from the results of the manufacturers' qualification tests, independent testing lab failure data, and data obtained from an extensive U.S. Corps of Engineers testing program. These data were statistically combined with the expert opinion survey data to produce fragility curves for the generic component categories.

A second useful source of fragility Information is a compilation of site-specific fragilities (Campbell et al., 1985) derived from past seismic PRAs prepared by Lawrence Livermore National Laboratory. By selecting a suite of site-specific fragilities for any particular component, one can obtain an estimate of a generic fragility for that component.

Following the probabilistic screening of the seismic accident sequences, plant-specific fragilities are developed for components not fitting in the generic database categories as determined during the plant visit. These are developed either by analysis or by an extrapolation of the seismic equipment qualification tests.

Building and component seismic responses (floor slab spectral accelerations as a function of acceleration) are computed at several peak ground acceleration values on the hazard curve. Three basic aspects of seismic response (best estimates, variability, and correlation) must be estimated.

For soil sites, SHAKE code calculations (Schnabel, Lysmer, and Seed, 1972) can be performed to assess the effect of the local soil column (if any) on the surface peak ground acceleration and to develop strain-dependent soil properties as a function of acceleration level. This permits an appropriate evaluation of the effects of nonhomogeneous underlying soil conditions that can strongly affect the building responses.

Building loads, accelerations, and in-structure response spectra can be obtained from multiple time history analyses using the plant design, fixed-base beam element models for the structures combined with a best-estimate model of the soil column underlying the plant.

14.2.4 Activity 4 — Quantification

Quantification proceeds through a process of convolution of the seismic hazard curves with the structures and component fragility curves to obtain probability of each element's failure under each discrete earthquake acceleration, along with integrated plant response and proper treatment of coupling due to the earthquake. Then, for each acceleration range, the failure probabilities due to the earthquake are propagated through the event tree/fault tree model along with the probabilities of independent failures. Essentially, for each discrete earthquake acceleration level, the quantification process follows the activities for the

internal events analysis. One of the fundamental distinctions is the integration of the exceedance frequency probability curve for seismic events into the overall results.

14.2.5 Additional Guidance

The theory behind, and practice involved with, performing a seismic PRA are well documented in the open literature and will not be replicated here. Papers that describe the methodology for conducting a seismic PRA for nuclear power plants (in particular, Ang and Newmark, 1977; and Kennedy, 1980) begin conceptually and then move to fully plant-specific analysis techniques. The SSMRP generated significant information that underpins much of the later work in this area (Smith et al., 1981). With the publication of the Zion and Indian Point Probabilistic Safety Studies (ComEd, 1981; ConEd, 1983), the basic approach became well established. More recently, the Diablo Canyon Long-Term Seismic Program (PG&E, 1988), performed by a U.S. utility company with strong review and direction provided by the U.S. Nuclear Regulatory Commission, extended the thoroughness of seismic PRA by including extensive testing and analysis involving all disciplines related to seismic risk. This detailed work led to improvements in the seismic PRA models and generally supported the idea that the basic modeling structure could be used to predict seismic failure of structures and components.

However, the usual practice in seismic PRA is still to employ outside experts to perform the seismic hazard and fragility analyses. These experts must work very closely with the PRA team to ensure that seismic failure modes of equipment imply functional failure as required for PRA models. Examples abound of PRA errors caused by the lack of communication between systems analysts and structural analysts.

14.3 Products

As identified in the task Documentation, the current task will produce draft material for the final report. Goals of this task include, as a minimum, the development of a seismic hazard curve, a listing of seisimically sensitive equipment and their fragility values, an identification of seismic-induced initiators and their frequencies, a listing of the seismic cutsets, and the quantification of the seismic-induced scenarios including the assignment of specific plant damage states. Specifically, this task will generate the following documentation:

1. Report documenting the seismic hazard curve and its basis (Activity 1).

2. Two Activity 2 letter reports: one letter report indicating the original equipment and structures list for inclusion in the fragility analysis, and a second letter report summarizing results of the walkdown (composition of the walkdown team and their areas of expertise, revisions to the equipment and structures list, changes projected in analysis requirements as a result of on-site observations). A final report by the structural analysis team documenting the fragility curves for plant structures and probabilistic safety assessment-related equipment and the details of the fragility analysis.

3. Final documentation: This is the seismic analysis appendix to the Main PRA Report. It fully documents the complete seismic PRA process, i.e., how the plant logic modeling team worked with the structural analysis team that produced the fragility analysis in defining equipment and structures to be analyzed, how the walkdown was conducted including how the structural analysts and systems analysts jointly screened equipment, how logic models were modified to incorporate structural failures and new equipment failure modes, summary presentations of the results of the seismic hazard and fragility analyses, and the results of quantification of the seismic PRA model.

14.4 References

Ang, A. H.-S. and N. M. Newmark, "A Probabilistic Seismic Assessment of the Diablo Canyon Nuclear Power Plant," Report to U.S. Nuclear Regulatory Commission, N.M. Newmark Consulting Engineering Services, Urbana, IL, November 1977.

Bernreuter, D. L., "Seismic Hazard Analysis: Application of Methodology, Results and Sensitivity Studies," NUREG/CR-1582, Lawrence Livermore National Laboratory, October 1981.

Bley, D. C., et al., "The Impact of Seismically Induced Relay Chatter on Nuclear Plant Risk," *Transactions of the Ninth International Conference on Structural Mechanics in Reactor Technology*, Vol. M, "Structural Reliability Probabilistic Safety Assessment," pp. 23-28, August 17-21, 1987.

Bohn, M. P., and J. A. Lambright, "Procedures for the External Events Core Damage Frequency Analysis for NUREG-1150," NUREG/CR-4840, Sandia National Laboratories, November 1990.

Budnitz, R. J., H. E. Lambert, and E. .E. Hill, "Relay Chatter and Operator Response after a Large Earthquake: An Improved PRA Methodology with Case Studies," NUREG/CR-4910, Future Resources Associates, Inc., August 1987.

Campbell, R. D., et al., "Seismic Risk Assessment of System Interactions," *Transactions of the Eighth International Conference on Structural Mechanics in Reactor Technology*, Brussels, Belgium, August 19-23, 1985.

ComEd, "Zion Probabilistic Safety Study," Commonwealth Edison Co., 1981.

ConEd, "Indian Point Probabilistic Safety Study," Consolidated Edison Co. and New York Power Authority, 1983.

IAEA, "Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants: A Safety Practice," Safety Series No. 50-P-7, International Atomic Energy Agency, 1995.

IAEA, "Probabilistic Safety Assessment for Seismic Events," IAEA-TECDOC-724, International Atomic Energy Agency, 1993.

Kaplan, S., V. M. Bier, and D. C. Bley, "A Note on Families of Fragility Curves—Is the Composite Curve Equivalent to the Mean Curve?" *Nuclear Engineering and Design*, 1992.

Kaplan, S., H. F. Perla, and D. C. Bley, "A Methodology for Seismic Risk Analysis of Nuclear Power Plants," *Risk Analysis*, Vol. 3, No. 3, September 1983.

Kennedy, R. P., et al., "Studies in Support of Fragility Analysis for Diablo Canyon Long-Term Seismic Program," Structural Mechanics Associates, 1988.

Kennedy, R. P., et al., "Probabilistic Seismic Safety Study of an Existing Nuclear Power Plant," *Nuclear Engineering and Design*, *59*, pp. 315-338, 1980.

Lambert, H.E., and R. J. Budnitz, "Relay Chatter and Its Effects on Nuclear Plant Safety," *Transactions of the Tenth International Conference on Structural Mechanics in Reactor Technology*, Los Angeles, California, August 1989.

PG&E, "Diablo Canyon Long Term Seismic Program," Pacific Gas and Electric Company, 1988.

Schnabel, P. B., J. Lysmer, and H. B. Seed, "SHAKE—A Computer Program for Earthquake Response Analysis of Horizontally Layered Sites," EERG-72-12, Earthquake Engineering Research Center, University of California at Berkeley, 1972.

Smith, P. D., et al., "Seismic Safety Margins Research Program - Phase I Final Report," NUREG/CR-2015, Vols. 1-10, Lawrence Livermore National Laboratory, 1981.

PART E - LEVEL 2/3 GUIDELINES

15. PROBABILISTIC ACCIDENT PROGRESSION AND SOURCE TERM ANALYSIS (LEVEL 2 PRA)

In this chapter, the analyses performed as part of the Level 2 portion of a probabilistic risk assessment (PRA) are described. A Level 2 PRA consists of five major parts:

1. Plant damage states,
2. Containment event tree analysis,
3. Release categorization
4. Source term analysis,
5. Severe accident management strategies.

Figure 15.1 shows the important relationships between this task and the other major tasks of the PRA. These relationships are discussed below in Section 15.1

15.1 Relation to Other Tasks

As identified in Figure 15.1, the current task requires information from several earlier PRA tasks. The Plant Familiarization task (Chapter 2) provides information important for the definition of plant damage states and the containment event tree analysis. This figure also indicates the importance of applying the principles of quality assurance in this task (refer to Chapter 4). The extent of the Level 2 analysis depends on the application as defined in the PRA Scope (Chapter 5). A listing of the frequencies and definitions of

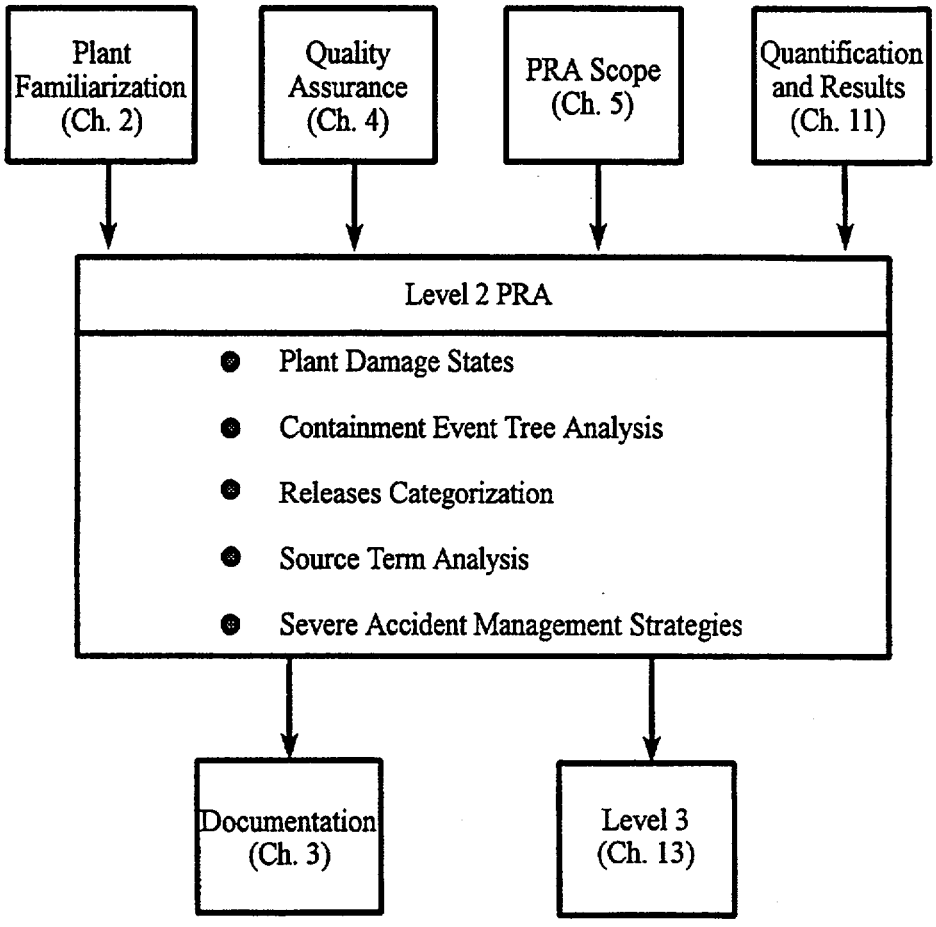


Figure 15.1 Relationships between Level 2 PRA and other tasks

importance of applying the principles of quality assurance in this task (refer to Chapter 4). The extent of the Level 2 analysis depends on the application as defined in the PRA Scope (Chapter 5). A listing of the frequencies and definitions of the core damage accident sequences determined in the Level 1 PRA is needed (Chapter 11).

Finally, depending upon the scope of the PRA (Chapter 5), the output of this task may be needed as input to a Level 3 PRA (Chapter 16). Also, output of this task goes to support the Documentation task (Chapter 3).

15.2 Task Activities

The purpose of this chapter is to provide a guide for assessment and management of severe accident risks in VVERs.

Probabilistic accident progression and source term analyses (Level 2 PRAs) address the key phenomena and/or processes that can take place during the evolution of severe accidents, the response of containment to the expected loads, and the transport of fission products from damaged core to the environment. Such analyses provide information about the probabilities of accidental radiological releases (source terms). The analyses also indicate the relative safety importance of events in terms of the possibility of offsite radiological releases, which provide a basis for development of plant-specific accident management strategies.

A concern associated with the results of Level 2 PRAs stems from their known susceptibility to phenomenological uncertainties. These uncertainties are often of such a magnitude that they make the decision-making process difficult. There is much to be gained, therefore, from assessment of severe accident risks, by reformulation of the Level 2 methodology into a simplified containment event tree (CET) and redefinition of the phenomenological portion in terms of a physically based probabilistic framework. Such an approach provides a streamlined procedure for assessment of severe accident risks that further allows for a direct evaluation of potential accident management strategies.

This document describes six major procedural activities for assessment and management of severe accident risks (see Figure 15.2). Section 15.2.1 provides guidance on development of plant damage states (PDSs) (Activity 1). Section 15.2.2 discusses the development of a simplified CET (Activity 2). The determination of the likelihood of occurrence of severe accident phenomena leading to various containment failure modes are also discussed in this section (Activity 3). Guidance is provided for deterministic analyses including consideration of uncertainties for severe accident issues. Section 15.2.3 discusses the accident progression grouping (source term categorization, Activity 4). Section 15.2.4 provides guidance on an evaluation of release and transport of radionuclides leading to an estimation of environmental source terms for each accident progression grouping (Activity 5). Output from Activity 5 provides the information needed to perform an offsite consequence assessment (Level 3 PRA). Chapter 16 provides guidance for performing a Level 3 PRA. Section 15.2.5 discusses the development of potential plant-specific accident management strategies to reduce the frequency of accident progression groups with large-release concerns (Activity 6). Appendix K describes the key phenomena and/or processes that can take place during the evolution of a severe accident and that can have an important effect on the containment behavior.

15.2.1 Plant Damage States

The role of interfaces between the system analysis (Level 1 PRA) and the containment performance analysis is particularly important from two perspectives. First, the likelihood of core damage can be influenced by the status of particular containment systems. Second, containment performance can be influenced by the status of core cooling systems. Thus, because the influences can flow in both directions between the system analysis and the containment performance analysis, particular attention must be given to these interfaces.

The Level 1 PRA analysis identifies the specific combination of system or component failures (i.e., accident sequence cutsets) which can lead to core damage. The number of cutsets generated

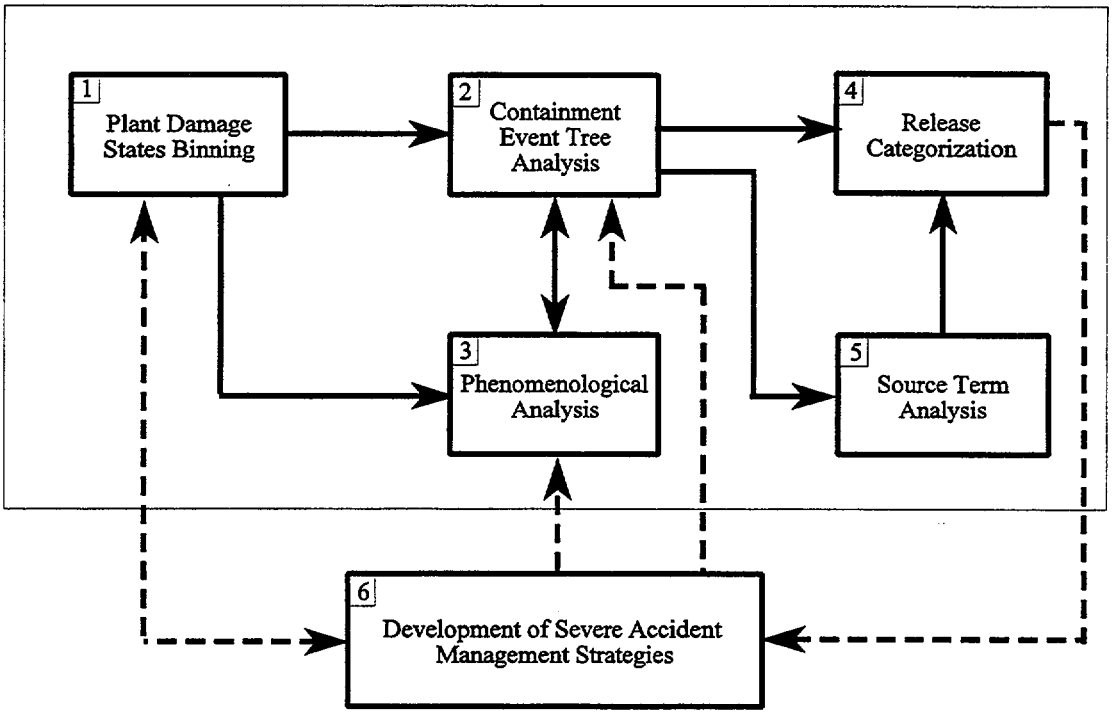


Figure 15.2 Major procedural activities for assessment and management of severe accident risks

by a Level 1 analysis is very large. It is neither practical nor necessary to assess the severe accident progression, containment response, and fission product release for each of these cutsets. As a result, the common practice is to group the Level 1 cutsets into a sufficiently small number of "plant damage states" to allow a practical assessment and management of severe accident risks.

A PDS should be defined in such a way that all accident sequences associated with it can be treated identically in the accident progression analysis. That is, the PDS definition must recognize all distinctions that matter in the accident progression analysis. It is clear that some PDSs will be more challenging to containment integrity than others. For example, some PDSs will completely bypass containment, such as accidents in which the isolation valves between the high-pressure reactor coolant system (RCS) and the low-pressure secondary systems fail causing a loss-of-coolant accident (LOCA) outside containment. Other examples include failure of the steam generator (SG) tubes and loss of containment isolation. Early loss of containment integrity can be the result of "internal" initiating events and can also be caused by "external" initiators (such as seismic events). In past PRAs for some U.S. plants, seismic initiators have been important contributors to the frequency of loss of containment isolation.

For those situations where the containment is initially intact, some PDS groups will cause more severe containment loads (e.g., elevated pressures and temperatures) than others. For example, a transient event with loss of coolant injection and containment heat removal (e.g., failure of containment sprays) will result in a core meltdown with the reactor coolant system at high pressure. A high-pressure core meltdown has the potential to cause more severe containment loads than say a LOCA with the containment heat removal systems operating. Accidents initiated by seismic events also tend to be important

contributors to the frequency of the severe PDS groups. This is because seismic events have the potential to cause multiple equipment failures and hence result in more severe PDS groups.

Before PDSs are defined, the analyst must identify plant conditions, systems, and features that can have a significant impact on the subsequent course of an accident. All potential combinations of the PDS characteristics that are physically possible are tabulated and assigned an identifier. The PDS matrix is usually developed by a Level 2 analyst and then reviewed by a Level 1 analyst for compatibility with the plant model and completeness in the appropriate dependencies. The matrix is revised, as necessary, until all requirements specified by the Level 1 and Level 2 analysts are deemed satisfactory. For example, the PDS should be defined such that it yields a unique set of conditions for entering the containment event tree. A Level 2 analyst may find it necessary or convenient to distinguish among groups of scenarios that have been assigned to a common PDS. This might be the case if distinct scenario types have been assigned to a particular PDS but subsequently prove to have different Level 2 signatures. The past experience of the Level 2 analyst helps to reconcile these issues.

All of the plant model information on the operability status of active systems that are important to the timing and magnitude of the release of radioactive materials must be passed into the CET via the definition of the PDS. Therefore, the plant model event trees must also address those active systems and functions that are important to containment isolation, containment heat removal, and the removal of radioactive material from the containment atmosphere. A containment spray system is a good example of such a system.

A relatively simple set of PDS attributes is, therefore, proposed in Table 15-1 that will identify those accidents that are more challenging to containment integrity than others. The attributes given in Table 15-1 allow the accident sequences generated in the Level 1 analysis for both "internal" and "external" events to be processed through the simplified CET described in Section 15.2.2. The VVER analysts should verify that the attributes given in Table 15-1 are appropriate and ask themselves whether VVERs have some other features that also belong on this table. It should also be noted that the PDS groups in Table 15-1 assume that seismic events will not cause any unique containment failure modes but simply influence the frequency of the more severe PDS groups. If unique failure modes are identified in the external event PRA, then Table 15-1 should be expanded accordingly.

15.2.2 Containment Event Tree Analysis

The evaluation of accident progression and the attendant challenges to containment integrity is an essential element of a risk assessment. The key phenomena and/or processes that can take place during the evolution of a severe accident and that can have an important effect on containment behavior are described in Appendix K (which is an update to Appendix 1 of NRC Generic Letter 88-20, 1988). The discussion in Appendix K identifies those issues that need to be considered when attempting to characterize the progression of severe accidents and the potential for various containment failure modes or bypass mechanisms. Of particular importance is to determine the effectiveness of those systems that are relied upon to mitigate the consequences of severe accidents. Appendix K lists some of the considerations that need to be addressed by the VVER analysts prior to taking credit for a system in the Level 2 PRA. In particular, it should be determined whether or not the equipment under consideration is qualified to operate successfully in the harsh environmental conditions (high temperature, pressure, humidity, radioactivity, aerosol concentration, etc.) associated with core meltdown accident. The discussion in Appendix K can be summarized by using event sequence diagrams such as those shown in Figures 15.3 and 15.4.

First, it is most important to determine the status of containment prior to core damage. Thus, the first event (in both diagrams) after accident initiation is to determine containment status. If the containment is bypassed or not isolated (Figure 15.3), then it is inevitable that radionuclides will be released to the environment after core damage. Therefore, the diagram focuses on those events that will influence the magnitude and timing of the release.

Table 15-1 Plant damage state attributes

Initiator Type	•Large, intermediate, or small LOCAs •Transients •Bypass events - Interfacing systems LOCA - Steam generator tube rupture (SGTR)
Status of Containment at Onset of Core Damage	•Isolated •Not isolated
Status of Containment Systems	•Sprays (if any) always operate/fail or are available if demanded •Sprays operate in injection mode, but fail upon switchover to recirculation cooling
Electric Power Status	•Available •Not available
Status of Reactor Core Cooling System	•Fails in injection mode •Fails in recirculation mode
Heat Removal from the Steam Generators	•Always operate/fail or are available if demanded •Not operating and not recoverable

Radionuclides released while the core is in the reactor vessel are termed "in-vessel release." accidents (such as interfacing systems LOCA), it is possible that the break location outside of containment is under water. If the radionuclides pass through such a pool of water, then significant "scrubbing" or retention of the aerosols can occur, which reduces the source term to the environment. Similarly, for an accident in which the containment is not isolated, containment sprays can significantly lower the airborne concentration of radionuclides with a corresponding reduction in the environmental source term.

It is important to determine if coolant injection can be restored and core melt arrested in the reactor vessel (as happened in the Three Mile Island Unit 2 accident) prior to vessel meltthrough. If core damage is not terminated in-vessel, it is important to know if the region under the vessel is flooded. A flooded cavity could cool the core debris and prevent core-concrete interactions (CCIs) (coolable debris bed) and eliminate radionuclide release from this mechanism (i.e., no ex-vessel release). However, if the cavity is dry, extensive CCIs can occur resulting in significant radionuclide release (i.e., ex-vessel release occurs) and the possibility of basemat meltthrough. It is also necessary to determine whether or not the flow path from the damage core to the environment is flooded or affected by spray operation.

Alternatively, if the containment is isolated and not initially bypassed, the event sequence diagram (Figure 15.4) focuses on identifying when the containment might fail or be bypassed during the cause of a severe accident. For clarity, only three potential release mechanisms are included in the diagram. An early release is defined as a release that occurs prior to or shortly after the core debris melts through the reactor vessel

An early release can be caused by several different failure mechanisms, which are discussed in Appendix K and will be explained in more detail later in this procedure guide. However, for the purposes of developing a simple event sequence diagram, it is known that these failure mechanisms are strongly influenced by the pressure in the reactor coolant system and whether or not core damage can be terminated by restoring coolant injection prior to vessel meltthrough. It is also possible that the damaged core can be retained in the reactor vessel by external cooling if the cavity is flooded.

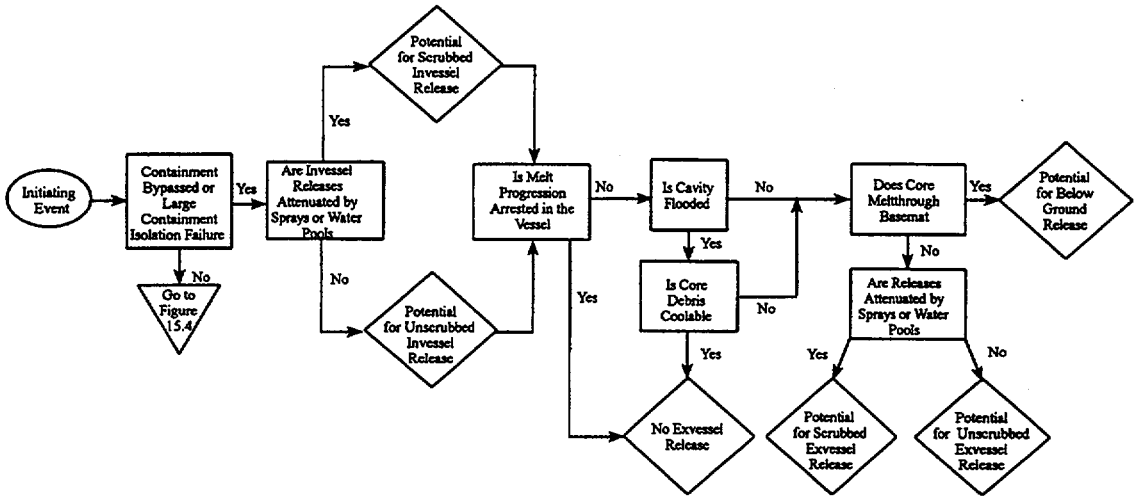


Figure 15.3 Event sequence diagram for accidents in which the containment is bypassed or not isolated

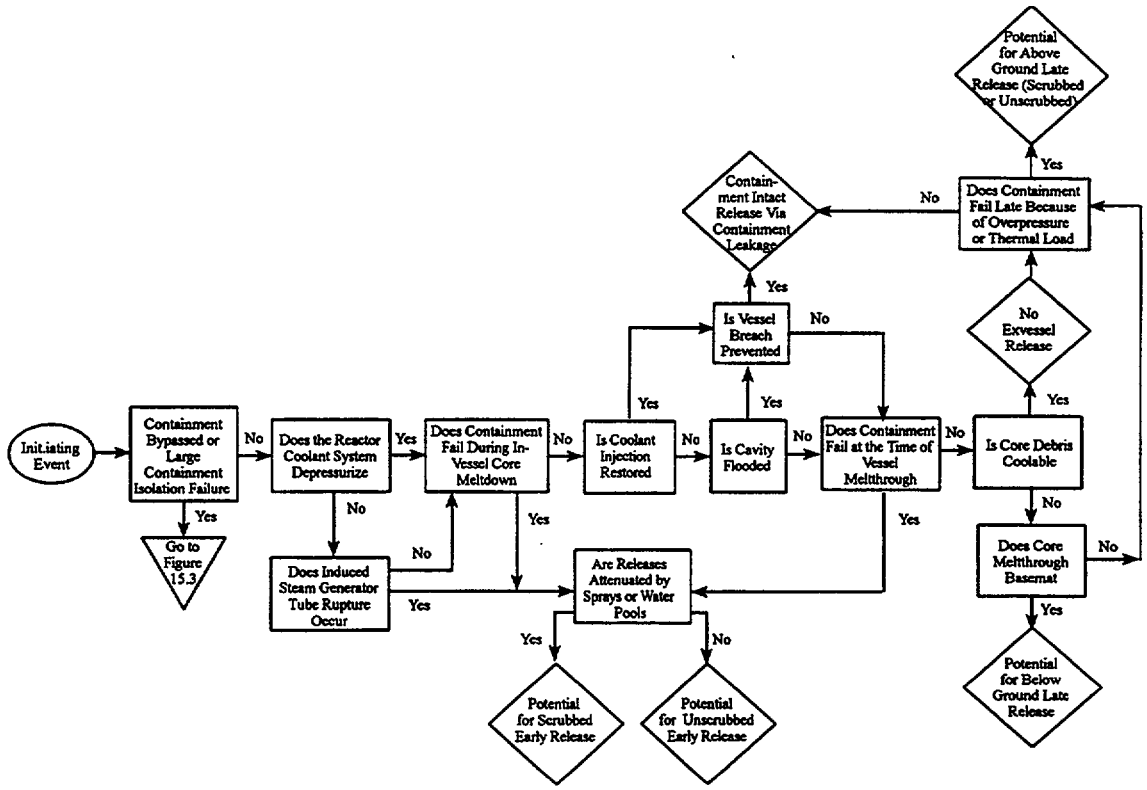


Figure 15.4 Event sequence diagram for accidents in which the containment is initially intact

If the core debris cannot be cooled and retained in the reactor vessel, the potential exists for containment failure at the time of reactor vessel meltthrough. If the containment does not fail "early," then the potential exists for late containment failure. In this context, "late" is defined as several hours to days after the core melts through the vessel. Late failure can occur as a result of high pressures or temperatures if active containment heat removal systems are not available. These types of failures are usually structural failures and can occur above ground. If the cavity is dry or the core is not coolable, late containment failure can occur as a result of the core debris melting through the concrete basemat. Under these circumstances, the release would be below ground. Of course, if the containment is not bypassed and does not fail (early or late), then the release to the environment will be via containment leakage. The VVER analysts should construct event sequence diagrams of the type shown in Figures 15.3 and 15.4 that reflect plant-specific features that have the potential to influence severe accident progression.

The next step in the process is to determine the probabilities of potential containment failure modes and bypass mechanisms conditional on the occurrence of each plant damage state identified in Section 15.2.1. This step is normally achieved by using event trees that incorporate events such as those shown in Figures 15.3 and 15.4 and address the issues discussed in Appendix K. A CET is a structured framework for organizing the different accident progressions that may evolve from the various core damage accident sequences. The top events in a CET are developed so that the likelihood of whether the containment is isolated, bypassed, failed, or remains intact can be determined. CETs can vary from relatively small trees with a few top events developed for each plant damage state group to very large and complex trees that are able to accommodate all plant damage states. An example of a simplified CET is provided in Table 15-2.

This CET is based on the event sequence diagrams in Figures 15.3 and 15.4 and also incorporates the issues discussed in Appendix K. The top events in the CET are the key attributes for a typical U.S. pressurized water reactor with a large-dry containment. The VVER analysts should verify the completeness of Table 15-2 and determine if VVER plants have some other features that should be incorporated into the CET.

Some of the CET questions correspond to the availability of various systems whereas other questions are related to the likelihood of physical phenomena leading to containment failure. For example, it is initially important to determine if the containment is isolated or bypassed (Question 1). This question can be answered based on information contained in the PDSs.

However, the likelihood of containment failure (Question 13) depends on quantifying uncertain phenomena which are, in turn, strongly influenced by the pressure (Question 6) in the reactor coolant system during core meltdown and vessel failure (refer to the discussion in Appendix K). In a similar manner, the issue of debris bed coolability (Question 15) is another important phenomenological issue that strongly influences the potential for containment failure (Question 16) in the late time frame.

Table 15-2 identifies those questions that can be quantified from system (and human) reliability analyses including consideration of potential severe accident management strategies (Questions 1, 2, 3, 4, 5, 6, 7, 10, 11, and 14) and those that require phenomenological analyses (Questions 8, 9, 12, 13, 15, and 16). An approach for dealing with each question in the CET is presented below. Quantification of those questions in the CET that deal with system (and human) reliability analyses are in part based on information contained in the PDS groups.

However, the PDS groups only provide information on which systems are potentially available for particular accident sequences. Whether or not the systems successfully operate during a severe accident has to be evaluated (refer to Appendix K) as part of the Level 2 PRA. In addition, any operator actions that are in the formal operating procedures for the plant should be included in the PRA. However, after core damage, there are a number of actions that an operator could take that could terminate and significantly mitigate the consequences of a core meltdown accident but which are not part of the operating procedures. Operator actions of this nature should be included in severe accident management strategies and should complement

Table 15-2 Nodal questions for a simplified CET

	Top Event Question	Prior Dependence	Question Type
1.	Is the containment isolated or not bypassed?	None	Based on PDS
2.	What is the status of reactor core cooling system?	None	Based on PDS
3.	Is power available?	None	Based on PDS
4.	Are the sprays actuated prior to reactor vessel meltthrough?	3	Based on PDS and accident management
5.	Is heat removal from the steam generators possible?	None	Based on PDS
6.	Does the reactor coolant system depressurize?	2, 3, 5	Based on PDS, design and accident management
7.	Is in-vessel coolant injection restored?	2, 3	Based on PDS and accident management
8.	Does thermally induced steam generator tube rupture occur?	6	Phenomena
9.	Does the containment fail prior to reactor vessel meltthrough?	1, 4, 6	Phenomena
10.	Is the break location under water for bypass accidents?	1, 2, 7	Based on PDS design and accident management
11.	Is the region under the reactor vessel flooded or dry?	2, 4	Based on PDS, design and accident management
12.	Is reactor vessel breach prevented?	6, 7, 11	Phenomena and design
13.	Does containment fail at vessel breach?	6, 8, 9	Phenomena
14.	Do the sprays actuate or continue to operate after vessel breach?	3, 4	Based on PDS and accident management
15.	Is the core debris in a coolable configuration?	4, 11	Phenomena
16.	Does containment fail late?	9, 11, 13, 14, 15	Phenomena

the normal plant operating procedures. The discussion below indicates where opportunities (in Questions 4, 6, 7, 10, 11, and 14) exist for implementing accident management strategies.

The analyst should first quantify the CET without the benefit of these accident management strategies. The CET can be readily requantified to assess the impact of any strategy on the likelihood of containment failure or bypass. Decisions related to implementing accident management strategies should be based on the integrated risk results. Section 15.2.5 describes some of the considerations that must be taken into account when developing these strategies.

The CET also includes several highly complex phenomenological issues associated with the progression of a core meltdown accident. A two-step approach is provided to assess the likelihood of various containment failure modes induced by these highly complex severe accident phenomena. As a first step, a relatively simple scoping analysis should be performed. If, however, the scoping analysis is inconclusive, then a more detailed second step would be needed. This second step is described below for some of the phenomenological questions in the CET.

Question 1 - Is the containment isolated or not bypassed?

This question can be answered based on information in the PDS. A negative response to this question includes accidents in which the containment fails to isolate as well as accidents that bypass containment (such as interfacing systems LOCA and SGTR). This question applies only to accidents in which the containment fails to isolate or is bypassed at or before accident initiation. Accident sequences that result in the containment becoming bypassed (such as induced SGTR) after core damage do not apply to this question. These accidents are included under the response to Question 8 below.

Question 2 - What is the status of reactor core cooling system?

This question can also be answered based on information in the PDS. If the coolant injection pump fails in the injection mode, then the contents of the water storage tanks will not be injected into containment (unless the containment spray operates). For some containment designs, the reactor cavity can only be flooded if the contents of the water storage tanks are injected into containment. The VVER analysts should ascertain whether or not this is also true for the VVER containment design under consideration. The response to this question influences the response to Question 11 below.

Question 3 - Is power available?

This question is answered from information in the PDS. The status of power availability is important for determining whether or not certain actions can be undertaken during the course of the accident. For example, spray system operation requires power (unless a dedicated power supply is provided) so that the response to this question directly influences the response to Questions 4 and 14. Power is also needed to depressurize the RCS (Question 6) and restore in-vessel coolant injection (Question 7).

Question 4 - Are the sprays actuated prior to reactor vessel meltthrough?

This question can be answered in part based on information in the PDS but can also be influenced by potential accident management strategies. Containment sprays can be automatically actuated based on a high containment pressure signal. Under these circumstances and if power is available, the spray system would be actuated early in the accident. However, it has been suggested that delaying spray operation to later times may be more beneficial from an accident management perspective. Other potential strategies involve the use of alternate water supply systems. Section 15.2.5.1 describes some of the considerations that need to be taken into account when developing accident management strategies related to containment spray operation. In addition, Appendix K stresses that it is also necessary to carefully assess whether or not a system will be able to perform the intended function under the harsh environmental conditions of a severe accident.

Question 5 - Is heat removal from the steam generators possible?

Information contained in the PDS can be used to determine if heat removal from the steam

generators is possible for each of the accident sequences under consideration. Heat removal from the steam generators is one possible way of depressurizing the RCS. Thus, the success of some accident management strategies designed to depressurize the RCS (refer to Question 6 and Section 15.2.5.2 below) are contingent on a positive response to this question.

Question 6 - Does the reactor coolant system depressurize?

For accidents initiated by transients and small break LOCA, the RCS will remain at high pressure unless the operators depressurize the RCS or induced failure of the RCS pressure boundary occurs (thermally induced SGTR is addressed under Question 8 below). For accidents initiated by intermediate and large break LOCA, the RCS will depressurize and be at low pressure prior to core damage. Thus, information in the PDS related to the initiator type (i.e., a transient event or a small break LOCA versus a large or an intermediate LOCA) can be used to answer this question.

However, it is generally recognized that if the RCS remains at high pressure (i.e., transients and small break LOCAs) during a core meltdown accident, the challenges to containment integrity will be more severe than for low-pressure sequences. Consequently, various accident management strategies have been proposed to depressurize the RCS for those accidents that would otherwise be characterized as high RCS pressure sequences. Depressurization can potentially be achieved by heat removal through the steam generators (positive response to Question 5) or by direct pressure relief of the RCS. Again, the ability of these systems to adequately depressurize the RCS during severe accident conditions needs to be carefully evaluated. However, prior to implementing RCS depressurization strategies, a number of adverse effects need to be considered as indicated in Section 15.2.5.2.

Question 7 - Is in-vessel coolant injection restored?

This question can be answered based on information in the PDS. At a minimum, power and water must be available in order to restore injection. In addition, for some accidents, the RCS must be depressurized (if only low head injection pumps are available) in order to restore coolant injection. Injecting water into a damaged reactor core is done to terminate core meltdown and establish a coolable geometry. Several accident management strategies have been proposed for injecting water into the RCS (refer to Section 15.2.5.3).

Question 8 - Does thermally induced steam generator tube rupture occur?

The likelihood of a temperature-induced creep rupture of the SG tubes depends on several factors including the thermal-hydraulic conditions at various locations in the primary and secondary systems, which determine the temperatures and the pressures to which the SG tubes are subjected as the accident progresses. Other relevant factors include the effective temperature required for creep rupture failure of the SG tubes and the presence of defects in the SG tubes which increase the likelihood of rupture.

Thermally induced SGTRs can occur after the SGs have dried out and very hot gas is circulating. The horizontal SG design in VVERs most likely precludes counter-current natural circulation flow in the hot leg. However, the possibility of water seal clearing at the bottom of the downcomer and at the cold leg loop seals is a potentially important issue for thermally induced failure of the SGs and should be studied for VVERs.

Question 9 - Does the containment fail prior to reactor vessel meltthrough?

This question deals with the likelihood of a hydrogen combustion event failing the containment prior to vessel failure. In order to determine the likelihood of failure, the magnitude of the pressure rise caused by a hydrogen combustion event has to be compared against the ultimate capacity of the containment. The ultimate capacity of the containment is usually a factor of 2.5 to 3 times the design pressure. In a separate project, the NRC is sponsoring research at the Russian Academy of Sciences in which a finite element model of the Kalinin containment is being developed. This model will be used to predict the response of the containment structure

to pressure loads in order to determine the ultimate pressure capacity. The results of this activity can be used to help quantify the CET for the Kalinin plant. It should be noted that in order to quantify the CET, a fragility curve (i.e., a probability of failure versus pressure curve) is needed. Developing these fragility curves require engineering judgment and information obtained from the finite element analysis and other sources. Examples of how fragility curves can be developed are given in Breeding et al. (1990) which describes how an expert panel addressed structural response issues.

The magnitude of the pressure loads caused by combustion events can be determined by a number of approaches. As a first step, the amount of hydrogen generated during in-vessel core meltdown can be estimated. The pressure rise from the combustion of this hydrogen can then be calculated by assuming adiabatic energy transfer to the containment atmosphere. If the containment can withstand this bounding adiabatic pressure load, then no further analysis for this potential failure mode is needed and the conditional probability of containment failure via this mechanism prior to reactor vessel meltthrough is zero. However, if the adiabatic load is close to or exceeds the containment capacity, then a more detailed analysis of this failure mechanism is needed.

The extent of containment loading due to hydrogen combustion is largely a function of the rate and magnitude of hydrogen production and the nature of the combustion of this hydrogen. Uncertainties associated with hydrogen loading arise from an incomplete state of understanding of various phenomena associated with hydrogen generation and combustion. These phenomena include in-vessel hydrogen generation, hydrogen transport and mixing, hydrogen deflagration, hydrogen detonation, and diffusion flames.

The issue regarding in-vessel hydrogen generation centers on the rate and quantity of hydrogen production and the associated hydrogen-steam mass and energy release rates from the RCS. These parameters strongly influence the flammability of the break flow, the containment atmosphere, and the magnitude, timing, and location of potential hydrogen combustion.

The degree of mixing and rate of transport of hydrogen in the containment building is an important factor in determining the mode of combustion. Hydrogen gas released during an accident can stratify, particularly in the absence of forced circulation and if there are significant temperature gradients in the containment. Hydrogen released with steam can also form locally high concentrations in the presence of condensing surfaces. Should the hydrogen accumulate in a locally high concentration, then flame acceleration and detonation could occur. Hydrogen mixing and distribution in a containment is sensitive to the hydrogen injection rate and the availability of forced circulation or induced turbulence in the containment. The results of large-scale hydrogen combustion tests performed at the Nevada Test Site appear to qualititatively support the notion that operating the spray system will result in a well-mixed atmosphere (Thomson, 1988).

Hydrogen deflagrations involve the fast reaction of hydrogen through the propagation of a burning zone or combustion wave after ignition. The combustion wave travels subsonically and the pressure loads developed are, for practical purposes, static loads. Deflagrations are the most likely mode of combustion during degraded core accidents. In fact, the deflagration of a premixed atmosphere of hydrogen-air-steam occurred during the Three Mile Island Unit 2 accident. The likelihood and nature of deflagration in containments is strongly influenced by several parameters--namely, composition requirement for ignition, availability of ignition sources, completeness of burn, flame speed, and propagation between compartments. In addition, combustion behavior is influenced by the effects of operating sprays.

Experimental studies of hydrogen combustion have been performed to understand the combustion behavior under expected plant conditions, and there is a reasonably complete database at several scales for ignition limits, combustion completeness, flame speed, and burn pressure for a hydrogen-steam-air mixture.

Improved correlations for flame speed and combustion completeness have been derived by Wong (1987). These correlations were derived based on the combustion data from the Variable Geometry Experimental System (Benedick,

Cummings, and Prassinos, 1982 and 1984); Fully Instrumental Test Series (Marshall, 1986); Nevada Test Site (Thomson, 1988); Acurex (Torok et al., 1983); and Whiteshell (Kumar, Tamm, and Harrison et al., 1984) experiments.

A physically based probabilistic framework like ROAAM (Theofanous, 1994) can be used to determine the uncertainty distribution for the peak pressure in the containment due to hydrogen combustion. The quasi-static loads from hydrogen combustion can be obtained by an adiabatic isochoric complete combustion model and then be corrected to account for burn completeness and expansion into nonparticipating compartments. The uncertainty distribution for hydrogen concentration and ignition frequencies should be used in the quantification of the pressure distribution for comparison with the ultimate pressure capability of the containment.

Question 10 - Is the break location under water for bypass accidents?

Core damage accident sequences that bypass containment (such as interfacing systems LOCA) usually result in significant fission product release to the environment. The relatively high environmental release for these accidents occurs because the release path bypasses attenuation mechanisms (such as sprays or water pools) that would otherwise be available to reduce the source term. A possible accident management strategy for containment bypass accidents is to flood the break location outside of containment (refer to Section 15.2.5.4) for those cases that would otherwise not be flooded.

Question 11 - Is the region under the reactor vessel flooded or dry?

This question can be answered by reference to the PDS. For example, in some containment designs if the water in the water storage tanks is injected into containment, then the reactor cavity will be flooded (i.e., a failure in the recirculation mode in Question 2). However, in other containment designs, accident management strategies are needed to ensure that sufficient water is injected into containment in order to flood the reactor cavity.

Flooding the reactor cavity can be beneficial during a core meltdown accident in two respects. First, a flooded cavity would externally cool the reactor vessel and (for some reactor designs) could prevent the core debris from melting through the bottom vessel head. This would prevent ex-vessel core debris interactions and the environmental consequences of the accident would be significantly reduced. Second, even if the core debris does meltthrough the vessel head, it could be cooled by the water in the cavity and if a coolable debris bed is formed, the potential for core-concrete interactions would be eliminated. Although a flooded cavity has obvious advantages, some of the potential adverse effects discussed in Section 15.2.5.1 need to be considered before implementing containment flooding strategies.

Question 12 - Is reactor vessel breach prevented?

This question deals with the likelihood of preventing vessel breach by retaining the core debris in the reactor vessel. This could be achieved in two ways--namely, by restoration of an in-vessel coolant injection (positive response to Question 7) or by externally cooling the lower head of the vessel (positive response to Question 11).

Accidents in which in-vessel coolant is restored within a certain time frame after the start of core damage can arrest the accident progression without vessel breach. For these accidents, subsequent questions related to containment failure at vessel breach are not pertinent. For a typical U.S. pressurized water reactor design, credit for in-vessel arresting of the accidents has been given for cases where water flow is restored within 30 minutes of the onset of the core damage. If cooling is restored within 30 minutes, the probability of successful arrest was assumed to be 1.0. A similar time frame appropriate for VVERs, based on core heatup characteristics and the potential for core coolability, should be developed.

The likelihood of preventing vessel breach by cavity flooding depends on several factors, such as the pressure in the primary system, the configuration of the cavity, the extent of submergence of the reactor vessel, and easy

access of water to the bottom of the reactor vessel. Under high RCS pressure circumstances, due to pressure and thermal loading, it is likely that vessel breach cannot be prevented by cavity flooding.

Under low RCS pressure circumstances, the likelihood of preventing vessel breach by external flooding can be evaluated by determining the thermal load distribution on the inside boundary of the lower head, the critical heat flux limitation on the outside boundary of the lower head (which is affected by the insulation) and the structural integrity of the lower head, when subjected to static and dynamic loads (i.e., fuel-coolant interactions). Detailed discussions and application of ROAAM to this issue for the Loviisa Nuclear Plant (VVER-440) in Finland and an advanced U.S. light water reactor (AP600) design can be found elsewhere (Tuomisto and Theofanous, 1994; and Theofanous et al., 1995). Some ideas to enhance the assessment basis as well as performance in this respect for application to larger and/or higher power density reactors are also provided by Theofanous et al. (1995).

Question 13 - Does containment fail at vessel breach?

The likelihood of containment failure at vessel breach depends on several factors, such as the pressure in the primary system, the amount and temperature of the core debris exiting the vessel, the size of the hole in the vessel, the amount of water in the cavity, the configuration of the cavity, and the structural capability of the containment building. Appendix K identifies the pressure in the RCS as the most important consideration for assessing the likelihood of containment failure at vessel breach. Therefore, this question depends heavily on the response to Question 6.

Low-Pressure Sequences

Under low RCS pressure circumstances, various mechanisms could challenge containment integrity. These include rapid steam generation caused by core debris contacting water in the cavity and hydrogen combustion. Again, scoping calculations can be performed to calculate bounding estimates of the pressure loads under these circumstances. These bounding pressure loads can be compared to the capacity of the containment building to determine the likelihood of failure. However, it is unlikely that these bounding pressure loads will exceed the ultimate capacity of the Kalinin containment. The probability of containment failure conditional on a low-pressure accident sequence is, therefore, expected to be relatively low (approximately 0.01) and driven by remote events, such as energetic fuel-coolant interactions of sufficient magnitude to project missiles through the containment structure. A recent report (Basu and Ginsberg, 1996) of a steam explosion review group presents an updated assessment of the likelihood of an in-vessel steam explosion causing containment failure. This report can be used as a basis for quantifying the CET.

High-Pressure Sequences

The most important failure mechanisms for high-pressure core meltdown sequences are associated with high-pressure melt ejection. Ejection of the core debris at high pressure can cause the core debris to form fine particles that can directly heat the containment atmosphere (i.e., direct containment heating [DCH]) and cause rapid pressure spikes. During high-pressure melt ejection, the hot particles could also ignite any combustible gases in containment, thereby adding to the pressure pulse. The potential for DCH to cause containment failure depends on several factors, such as the primary system pressure, the size of the opening in the vessel, the temperature and composition of the core debris exiting the vessel, the amount of water in the cavity, and the dispersive characteristics of the reactor cavity. Simple bounding calculations for high-pressure sequences are unlikely to be conclusive (i.e., they will almost certainly exceed the ultimate capability of the containment). Therefore, a more detailed analysis of this failure mechanism is needed.

Discussions on application of ROAAM to this issue is reported in "The Probability of Containment Failure by Direct Containment Heating in Zion," and its supplement (Pilch, Yan, and Theofanous, 1994). The basic understanding upon which the approach to quantification of DCH loads is based is that intermediate compartments trap most of the debris dispersed from the reactor cavity and that the thermal-chemical interactions during this dispersal process are limited by the incoherence in the steam blowdown and melt entrainment processes. With this understanding,

it is possible to reduce most of the complexity of the DCH phenomena to a single parameter: the ratio of the melt entrainment time constant to the system blowdown time constant which is referred to as the coherence ratio.

DCH loads also depend on parameters that characterize the system initial conditions, primary system pressure, temperature and composition (i.e., hydrogen mole fraction), melt quantity and composition (i.e., zirconium and stainless steel mass fraction), and initial containment pressure and composition. The key component of the framework, therefore, is the causal relations between these parameters and the resulting containment pressure (and temperature). Of these parameters, some are fixed, some vary over a narrow range, and some are so uncertain that they can be approached only in a very bounding sense. Plant-specific analyses should be performed to quantify the probability density functions for the initial melt parameters. However, sequence uncertainties can be enveloped by a small number of splinter scenarios without assignment of probability. These distribution functions, combined with a two-cell equilibrium model for containment, can be used to obtain a probability density function for the peak containment pressure.

The resulting distribution for peak containment pressure is then combined with fragility curves (probabilistically distributed themselves) for the containment structure to obtain a probability distribution of the failure frequency (Pilch et al., 1996). NUREG/CR-6338 (Pilch et al., 1996) provides further discussion on how the methodology and scenarios described in (Pilch, Yan, and Theofanous, 1994) were used to address the DCH issue for 34 Westinghouse plants with large volume containments. This report could be helpful for extrapolating the approach to a VVER containment.

Question 14 - Do the sprays actuate or continue to operate after vessel breach?

This question depends in part on the information in the PDS but is also influenced by accident management considerations. For some accident sequences, power is available and the sprays will continue to operate during recirculation. In other accident sequences, power will be restored and accident management strategies are needed to ensure the spray operation is restored in an appropriate manner. Section 15.2.5.1 provides guidance on developing accident management strategies for spray operation.

Question 15 - Is the core debris in a coolable configuration?

This question addresses the likelihood of coolability of the core debris released into the reactor cavity. Coolability of the core debris requires that the cavity region under the vessel be flooded (response to Question 11) and that the molten core materials are fragmented into particles of sufficient size to form a coolable configuration. Debris bed coolability is an important issue because if the debris forms a coolable geometry, the only source for containment pressurization will be the generation of steam from boiloff of the overlying water. Under these circumstances, if containment heat removal systems are available, then late containment failure would be prevented. Even in the absence of containment heat removal, pressurization from water boiloff is a relatively slow process and would result in very late containment failure allowing time for remedial actions. Furthermore, a coolable debris geometry would limit penetration of the core debris into the basemat and thus prevent this potential failure mode. This, in turn, limits CCIs and prevents radionuclide releases from the core debris (i.e., no ex-vessel fission product release).

There is, however, a significant likelihood that, even if a water supply is available, the core debris will not be coolable and, therefore, will attack the concrete basemat. Under these circumstances, noncondensible gases would be released in addition to steam and add to containment pressurization. Also, if significant CCI occurs, the core debris could penetrate the basemat (depending on the thickness of the concrete) and ex-vessel radionuclide release will occur.

Formation of a coolable debris bed depends on several factors, such as the mode of contact between the core debris and water, the size distribution of the core debris particles, the depth of the debris bed, and the water pool. As a general rule, unless the debris bed is calculated to be thin, both a coolable and noncoolable

configuration should be considered for the purposes of CET quantification.

Question 16 - Does containment fail late?

This question deals with the likelihood of containment failure long after vessel breach. The likelihood and timing of the late containment failure depends on the presence of water in the cavity (response to Question 11), core debris coolability (response to Question 15), and the availability of containment heat removal systems (response to Question 14). Each possible combination of responses is discussed below.

Dry Cavity

If the cavity is dry, the core debris will in general not be coolable and Question 15 is irrelevant. Extensive CCI will occur and noncondensible gases, steam and radionuclides will be released to containment. Containment pressurization rates can be obtained by simplified energy balance calculations assuming bounding values. In addition, combustible gases (H_2 and CO) will also be released during CCI and could result in combustion events. The impact of combustion can be evaluated in a manner similar to the approach discussed in Question 9. Furthermore, the likelihood of basemat penetration resulting from CCI should also be evaluated for the dry cavity case. The projected consequences of basemat meltthrough are, however, relatively minor compared with an above-ground failure of the containment that might be caused earlier by a combustion event or high-pressure loads.

Flooded Cavity

If the cavity is flooded, then the response to Question 15 (core debris coolability) is very important to CET quantification. Each possibility is discussed below.

Core debris coolable. If the core debris is coolable, CCI does not occur and all of the decay heat goes into boiling water. If the containment heat removal systems are operating, then late containment failure by overpressurization will be prevented. Also penetration of the basemat by the core debris will be prevented. If the containment heat removal systems are not operating, then containment failure will eventually occur unless remedial actions are taken.

Core debris uncoolable. If the core debris is not coolable, CCI will occur and the impact of noncondensible and combustion gases will have to be taken into account for CET quantification. In addition, the potential for basemat meltthrough will also have to be assessed.

15.2.3 Release Categorization

The CET analysis generates conditional probabilities for a large number of end states (i.e., potential ways in which radioactivity could be released to the environment). Some of these end states are either identical or similar, in terms of key radionuclide release characteristics. These end states are, therefore, grouped to a smaller number of release categories.

These release categories, which are often referred to as release bins or source term bins, should be defined on the basis of appropriate attributes that affect radiological releases and potential offsite consequences. These attributes are plant specific but should include:

- timing and size of containment failure or bypass
- operation of sprays (if operating what is the spray duration time)
- whether or not the core debris is flooded (if flooded is a coolable debris bed formed)
- whether or not the RCS is depressurized prior to vessel breach
- whether or not vessel breach is prevented (if vessel breach is prevented, ex-vessel release is also prevented)
- whether or not the break location is above or below ground level
- whether or not the break location is under water for bypass events.

15.2.4 Source Term Analysis

The magnitude and composition of radioactive materials released to the environment and the associated energy content, time, release elevation, and duration of release are collectively termed the "source term." The source term analysis tracks the release and transport of the radioactive materials from the core, through the RCS, then to the containment and other buildings, and finally into the environment. The removal

and retention of radioactive materials by natural processes, such as deposition on surfaces, and by engineered safety systems, such as sprays, are accounted for in each location.

For the analysis of source terms, a simple parametric approach is recommended similar to that used in NUREG/CR-5747 (Nourbakhsh, 1993). This method describes source terms as the product of release fractions and transmission factors at successive stages in the accident progression. The parameters entering this source term formulation can be derived from existing databases supplemented by a few plant-specific code calculations (e.g., using the MELCOR code). Using the resulting simplified formulation, a set of source terms that will have a one-to-one correspondence with each of the source term categories (see Section 15.2.3) can be obtained.

15.2.5 Development of Severe Accident Management Strategies

Severe accident management strategies consist of those actions that are taken during the course of an accident to prevent core damage, terminate core damage progression (and retain the core within the vessel), maintain containment integrity, and minimize offsite releases. Severe accident management strategies also involve preplanning and preparatory measures for severe accident management guidance and procedures, equipment and design modifications, and severe accident management training.

The assessment methodology discussed in Sections 15.2.1 through 15.2.5 provides a basis for the development and evaluation of potential plant-specific accident management strategies. The integrated results of procedural activities 1 to 5 (Figure 15.2) will be a set of accident progression groups (release categories) with corresponding frequency and radionuclide release characteristics (source term). Potential accident management strategies can then be developed to reduce the frequency of (or eliminate) accident progression groups with large release concerns.

All accident recovery/management actions should remain consistent between the Level 1 PRA and the CET analyses. The recovery actions prior to initiation of core damage (prevention strategies) should be credited in the Level 1 PRA, while any actions beyond the initiation of core damage (post-core damage accident mitigation) should be evaluated as a part of the Level 2 PRA assessment.

The simplified containment event tree discussed in Section 15.2.2 (refer to Table 15-2) identified a number of opportunities for implementing accident management strategies. The severe accident management strategies identified are:

- spray or injection of water into containment (Questions 4, 11, and 14)
- RCS depressurization (Question 6)
- in-vessel water addition to a degraded core (Question 7)
- flooding the break location for bypass events (Question 10).

Careful evaluation of the feasibility and the relative advantages and disadvantages of each of these accident management strategies is needed prior to their implementation at any specific plant. Plant layout and geometry, the capacity and redundancy of emergency plant systems, as well as specific balance of plant features, can determine whether a particular strategy is feasible or makes sense under a certain accident scenario at a particular plant. For instance, containment pressure capability, areas for debris spreading, size of sumps, elevation of the reactor vessel, reactor cavity geometry and elevation, water storage tank capacities, flow rates of safety and nonsafety injection systems, and number of equipment trains are only a few of the items which will influence the decisions to be made at a specific site with regard to severe accident management. For further discussions on the results of severe accident management research and implementation, refer to the Organization for Economic Co-operation and Development report entitled, "Implementing Severe Accident Management in Nuclear Power Plants," (OECD, 1996).

15.2.5.1 Spray or Injection of Water into Containment

The use of the spray system or other means to inject water into containment is a potential severe accident management strategy (Questions 4, 11,

and 14) for all three time frames considered in the CET in Section 15.2.2. Containment sprays can have a number of beneficial effects on severe accident progression. There are, however, a number of potentially adverse effects, which should be considered before implementing a containment spray strategy at a particular plant. The pros and cons associated with spray operation during a severe accident are described below for each potential strategy.

Controlling Containment Atmosphere

Containment sprays can be used to cool and depressurize the containment atmosphere and thus prevent overpressure failure of the containment. Sprays can also remove fission products from the containment atmosphere so that if containment integrity is lost, the environmental source term will be lower than it would otherwise have been without the effect of sprays.

A potential adverse effect of restoring containment spray operation during the later stages of an accident is the deinerting of a previously steam-inerted atmosphere. This could produce conditions that would allow combustion of a large quantity of hydrogen. Consequently, any strategy to restore containment spray operation late in an accident sequence should consider the impact of hydrogen combustion.

External Cooling of the Reactor Vessel

In some containments, external flooding of the reactor vessel is feasible if sufficient water is injected into containment. This would provide an external heat sink for the reactor vessel and could reduce the boiloff of the in-vessel coolant. In many designs, the vessel lower head could be protected via external flooding, and this external cooling could prevent or delay vessel failure. By preventing the core debris from melting through the vessel lower head, this accident management strategy would eliminate ex-vessel interactions between the core and water and/or concrete.

A potential adverse effect associated with this strategy is that if vessel failure does occur, then accumulated water could interact with the molten core debris. These fuel-coolant interactions are likely to be accompanied by rapid steam generation and additional hydrogen production. While these interactions could be energetic, they are unlikely to threaten containment integrity. Nevertheless, the impact of fuel-coolant interactions should be considered prior to implementing a containment flooding strategy.

Flooding Ex-Vessel Core Debris

In some designs, adding or redistributing water to the containment prior to vessel failure could protect against containment failure by such mechanisms as direct attack of the containment boundary or containment penetrations. If water is added after vessel failure and debris ejection, it can, depending on the design, provide a heat sink for the debris and a water pool to scrub fission products.

A potential adverse effect of this strategy is the steam production resulting from the interaction of sprayed or injected water with core debris. This interaction can be substantial depending on the water flow rate and the relative timing of water addition and debris addition into the containment. The amount of steam generated by molten core debris entering a water pool depends on pool depth and whether or not the debris is quenched. The threat posed by steam production to containment integrity will very much depend on the previously existing containment pressure and on the status of containment heat removal mechanisms. In addition, if external water sources are sprayed or injected into the containment, water could accumulate and may lead to flooding of vital containment areas reducing or eliminating containment heat removal or the pressure suppression function in some containments.

15.2.5.2 Reactor Coolant System Depressurization

RCS depressurization (Question 6 in the CET) can be accomplished via relief valves or via heat removal through the SGs. Regardless of the method used, RCS depressurization provides many positive responses to severe accidents but may also involve some undesirable effects.

RCS depressurization increases the opportunity for injecting water into the RCS from a number of low pressure sources. These include the designed low-pressure safety injection systems, accumulator tanks, and other, unconventional

sources, such as fire water systems. Besides providing opportunity for additional injection sources, RCS depressurization reduces the stress on the entire RCS and thus reduces the likelihood of unintentional failure of this fission product barrier including containing bypass via SGTR. Depressurization will also reduce the natural circulation flows in the reactor pressure vessel and steam generators tubes, thereby reducing thermal loads in both components. Depressurization also decreases the driving potential for high-pressure melt ejection if the core debris eventually melts through the vessel head.

On the negative side, depressurization through the relief valves will increase the rate at which hydrogen is discharged into the containment and could, depending on the depressurization rate, increase core oxidation and degradation. Also, if the RCS pressure is reduced, the potential for triggering energetic in-vessel fuel-coolant interactions is increased, but it is considered unlikely that such energetic interactions would fail the reactor pressure vessel.

Depressurization via the relief valves would increase the flow of fission products into the containment and reduce the time available for deposition of fission products in the RCS. For a containment with an isolation failure, depressurization of the RCS would increase containment pressure and lead to larger flows through the isolation breach. For a bypassed containment, RCS depressurization would decrease the flow through the bypass failure.

If RCS depressurization is accomplished via steam generator heat removal, then special consideration must be given to protect steam generator tube integrity. RCS pressurization will tend to increase the pressure difference across the steam generator tubes and, therefore, could lead to a tube failure or increase an already existing leak. This is especially true after core melt has occurred and the SG tubes are at high temperature. Also, since SG depressurization will increase the heat transfer in the tubes, hydrogen may concentrate there and impair the heat transfer process and limit the amount of RCS depressurization achievable. Injection of water into the secondary side of the steam generators would be expected to occur as they depressurize. This would further increase the heat transfer from the primary to the secondary side and enhance RCS depressurization. However, injection of cold water on the secondary side would increase the thermal stresses on the SG tubes and could lead to rupture and containment bypass. Obviously, this possibility decreases at higher water temperatures and lower flow rates. In addition, the presence of water on the secondary side would scrub fission products which have leaked from the primary to the secondary side.

15.2.5.3 In-Vessel Water Addition to a Degraded Core

Water addition to a degraded core may cool the core debris and lead to a safe, stable state. The consensus of the reactor safety community is that even if there are indications of a damaged reactor core, water should be injected when it becomes available. However, there may be a number of undesirable effects accompanying this action that plant personnel should be aware of and prepared for beforehand. These effects include the generation of steam as well as hydrogen plus the possibility of the core materials returning to a critical state. The successful termination of the accident as well as the extent and relative importance of the related phenomena depend on the timing and rate of the water addition and whether the water source is borated or unborated.

During the early stages of core damage, large amounts of water would rapidly quench the overheated core. Some steam would be produced but would be unlikely to substantially pressurize the RCS or produce large amounts of hydrogen. Smaller rates of water addition would lead to a slower quenching, additional hydrogen would be generated, and embrittled fuel and cladding could be shattered. At very small rates of water addition, quenching may not be achieved and substantial hydrogen could be generated with accident progression being accelerated.

For a badly damaged core, which is still within the RCS, similar consideration to those above would also apply. However, whether even large water flow rates can quench the core debris will depend on the specific geometry of the reconfigured debris. Furthermore, if there is a compact debris bed, its porosity and, therefore, its coolability may be reduced by the eventual distillation of the boron or other materials in the water.

After the core debris has melted through the reactor vessel, water injected in-vessel would help to minimize fission product revaporization and cool debris remaining in the vessel. In addition, water flowing out of the break in the lower vessel head would help to cool debris in the reactor cavity and perhaps reduce containment gas temperatures. In the long term, this water could quench the debris and arrest CCI. Again, whether the ex-vessel debris would be quenched depends on the flow rate of the water and the configuration of the debris. Water would also help to scrub volatile and nonvolatile fission products released from the fuel.

Water addition to the ex-vessel core debris also has implications for containment integrity. Depending on the water flow rate, significant steam generation and consequent containment pressurization can result. Additional hydrogen generation within containment can take place. Continued injection into the containment from outside (i.e., not normal emergency cooling system sources) may lead to flooding of containment areas where critical equipment resides. The fact that different water flow rates can lead to a decrease (because of quenching and termination of steam generation) or increase (because of steam, hydrogen production, and gas space compression) in containment pressure has particular significance for an unisolated or bypassed containment.

15.2.5.4 Flooding the Break Location for Bypass Events

This severe accident management action is aimed at providing fission product scrubbing. A water source, such as service water, could be used if the break location can be identified and a connection to the water system is available. An adverse effect of this strategy is that flooding could impact the operation of equipment located near the site of break.

15.3 Products

In general, sufficient information should be provided in the documentation to allow an independent analyst to reproduce the results. At a minimum, the following should be provided:

- a thorough description of the procedure used to group (bin) individual accident cutsets into PDSs, or other reduced set of accident scenarios for detailed Level 2 analysis,
- a listing of the specific attributes or rules used to group cutsets, and
- a listing and/or computerized database providing cross reference for cutsets to PDSs and vice versa.

Documentation of containment system performance assessments should include a description of information used to develop containment systems' analysis models and link them with other system reliability models. This documentation should be prepared in the same manner as that generated in the Level 1 analysis of other systems.

Documentation of analyses of severe accident progression should include the following:

- a description of plant-specific accident simulation models including extensive references to source documentation for input data,
- a listing of all computer code calculations performed and used as a basis for quantifying any event in the containment probabilistic logic model including a unique calculation identifier or name, a description of key modeling assumptions or input data used, and a reference to documentation of calculated results. (If input and/or output data are archived for quality assurance records or other purposes, an appropriate reference to calculation archive records is also provided.),
- a description of key modeling assumptions selected as the basis for performing "base case" or "best estimate" calculations of plant response and a description of the technical bases for these assumptions,
- a description of plant-specific calculations performed to examine the

effects of alternate modeling approaches or assumptions,

- if analyses of a surrogate (i.e., "similar") plant are used as basis for characterizing any aspect of severe accident progression in the plant being analyzed, references to, or copies of, documentation of the original analysis, and a description of the technical basis for assuring the applicability of results, and
- for all other original engineering calculations, a sufficiently complete description of the analysis method, assumptions, and calculated results is prepared to accommodate an independent (peer) review.

In general, sufficient information in the documentation of analyses performed to establish quantitative containment performance limits is provided that allows an independent analyst to reproduce the results. At a minimum, the following information is documented for a PRA:

- a general description of the containment structure including illustrative figures to indicate the general configuration, penetration types and location, and major construction materials,
- a description of the modeling approach used to calculate or otherwise define containment failure criteria,
- if computer models are used (e.g., finite element analysis to establish overpressure failure criteria), a description of the way in which the containment structure is nodalized including a specific discussion of how local discontinuities, such as penetrations, are addressed, and
- if experimentally determined failure data are used, a sufficiently detailed description of the experimental conditions to demonstrate applicability of results to plant-specific containment structures.

The following documentation is generated to provide the results and describe the process by which the conditional probability of containment failure is calculated:

- tabulated conditional probabilities of various containment failure modes with specific characterizations of time phases of severe accident progressions (e.g., early vs. late containment failures),
- a listing and description of the structure of the overall logic model used to assemble the probabilistic representation of containment performance (graphical displays of event trees, fault trees, or other logic formats are provided to illustrate the logic hierarchy and event dependencies),
- a description of the technical basis (with complete references to documentation of original engineering analyses) for the assignment of all probabilities or probability distributions with the logic structure,
- a description of the rationale used to assign probability values to phenomena or events involving subjective, expert judgment, and
- a description of the computer program used to exercise the logic model and calculate final results.

Documentation of analyses performed to characterize radiological source terms should provide sufficient information to allow an independent analyst to reproduce the results. At a minimum, the following information should be documented in a PRA:

- the radionuclide grouping scheme used and the assumptions made to obtain it should be clearly described, and
- the time periods considered for the release and the rationale for the choices made.

Documentation of analyses performed to characterize radiological source terms should

provide sufficient information to allow an independent analyst to reproduce the results. At a minimum, the following information should be documented in a PRA:

- a summary of all computer code calculations used as the basis for estimating plant-specific source terms for selected accident sequences, specifically identifying those with potential for large releases,
- a description of modeling methods used to perform plant-specific source term calculations; this includes a description of the method by which source terms are assigned to accident sequences for which computer code calculations were not performed,
- if analyses of a surrogate (i.e., "similar") plant are used (as a basis for characterizing any aspect of radionuclide release): transport or deposition in the plant being analyzed, references to, or copies of documentation of the original analysis, and a description of the technical basis for assuming applicability of results.

Documentation of analyses performed to characterize radiological source terms should provide sufficient information to allow an independent analyst to reproduce the results. At a minimum, a description of the method by which uncertainties in source terms are addressed should be documented for a quality PRA.

15.4 References

Basu, S. and T. Ginsberg, "A Reassessment of the Potential for an Alpha-Mode Containment Failure and a Review of the Current Understanding of Broader Fuel-Coolant Interaction Issues," NUREG-1524, U.S. Nuclear Regulatory Commission, August 1996.

Benedick, W. B., J. C. Cummings, and P. G. Prassinos, "Combustion of Hydrogen:Air Mixtures in the VGES Cylindrical Tank," NUREG/CR-3273, Sandia National Laboratories, 1984.

Benedick, W. B., J. C. Cummings, and P. G. Prassinos, "Experimental Results from Combustion of Hydrogen:Air Mixtures in an Intermediate-Scale Tank," Proceedings of the Second International Conference on the Impact of Hydrogen on Water Reactor Safety, NUREG/CP-0038, Sandia National Laboratories, 1982.

Breeding, R. J., et al., "Evaluation of Severe Accident Risks: Quantification of Major Input Parameters, Experts: Determination of Structural Response Issues," NUREG/CR-4551, Volume 2, Part 3, Sandia National Laboratories, October 1990.

Kumar, R. K., H. Tamm, and W. C. Harrison, "Intermediate-Scale Combustion Studies of Hydrogen-Air-Steam Mixtures," EPRI NP-2955, Electric Power Research Institute, 1984.

Marshall, B. W., "Hydrogen:Air:Steam Flammability Limits and Combustion Characteristics in the FITS Vessel," NUREG/CR-3468, Sandia National Laboratories, 1986.

Nourbakhsh, H. P., "Estimate of Radionuclide Release Characteristics into Containment Under Severe Accident Conditions," NUREG/CR-5747, Brookhaven National Laboratory, November 1993.

NRC, "Individual Plant Examination for Severe Accident Vulnerabilities - 10 CFR 50.54(f)," Generic Letter No. 88-20, U.S. Nuclear Regulatory Commission, November 23, 1988.

OECD, "Implementing Severe Accident Management in Nuclear Power Plants," Organisation for Economic Co-operation and Development, Nuclear Energy Agency, 1996.

Pilch, M. M., et al., "Resolution of the Direct Containment Heating Issue for all Westinghouse Plants with Large Dry Containment of Subatmospheric Containment," NUREG/CR-6338, Sandia National Laboratories, February 1996.

Pilch, M. M., H. Yan, and T. G. Theofanous, "The Probability of Containment Failure by Direct Containment Heating in Zion," NUREG/CR-6075, Sandia National Laboratories, 1994.

Theofanous, T. G., et al., "In-Vessel Coolability and Retention of Core Melt," DOE/ID-10460, July 1995.

Theofanous, T. G., "Dealing with Phenomenological Uncertainty in Risk Analysis," Workshop I in Advanced Topics in Reliability and Risk Analysis, Annapolis, MD, October 20-22, 1993, NUREG/CP-0138, October 1994.

Thomson, R. T., "Large-Scale Hydrogen Combustion Experiments, Volume 1: Methodology and Results," EPRI NP-3878, Electric Power Research Institute, October 1988.

Torok, R., et al., "Hydrogen Combustion and Control Studies in Intermediate Scale," EPRI NP-2953, Electric Power Research Institute, 1983.

Tuomisto, H. and T. G. Theofanous, "A Consistent Approach to Severe Accident Management," *Nuclear Engineering and Design, 148,* 171-183, 1994.

Wong, C. C., "HECTR Analysis of Nevada Test Site (NTS) Premixed Combustion Experiments," SAND87-0956, Sandia National Laboratories, 1987.

16. CONSEQUENCE ANALYSIS AND INTEGRATED RISK ASSESSMENT (LEVEL 3 PRA)

In this chapter, the analyses performed as part of the Level 3 portion of a probabilistic risk assessment (PRA) are described. A Level 3 PRA consists of two major parts:

1. Consequence analyses conditional on various release mechanisms (source terms) and
2. Computation of risk by integrating the results of Levels 1, 2, and 3 analyses.

Figure 16.1 shows the important relationships between this task and the other major tasks of the PRA. These relationships are discussed below in Section 16.1.

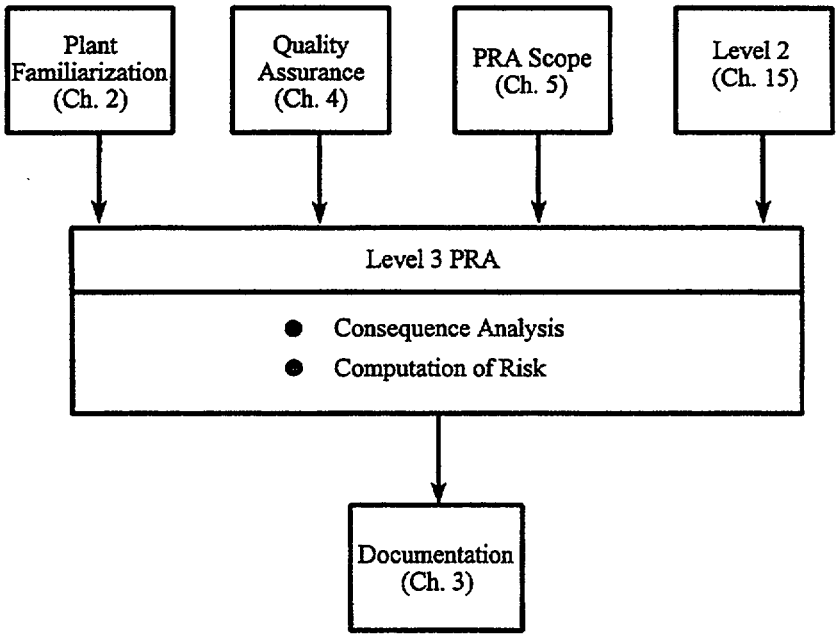


Figure 16.1 Relationships between Level 3 PRA and other tasks

16.1 Relation to Other Tasks

As identified in Figure 16.1, the current task requires a set of release fractions (or source terms) from the Level 2 analysis (Chapter 15) as input to the consequence analysis. The consequences are calculated in terms of: (1) the acute and chronic radiation doses from all pathways to the affected population around the plant, (2) the consequent health effects (such as early fatalities, early injuries, and latent cancer fatalities), (3) the integrated population dose to some specified distance (such as 50 miles) from the point of release, and (4) the contamination of land from the deposited material. The consequence measures to be calculated depends on the application as defined in PRA Scope (Chapter 5). Generally, in a Level 3 analysis, a distribution of consequences is obtained by statistical sampling of the weather conditions at the site. Each set of consequences, however, is conditional on the characteristics of the release (or source term) which are evaluated in the Level 2 analysis.

An integrated risk assessment combines the results of the Levels 1, 2, and 3 analyses to compute the selected measures of risk in a self-consistent and statistically rigorous manner. The risk measures usually selected are: early fatalities, latent cancer fatalities, population dose, and quantitative health objectives (QHOs) of the

U.S. Nuclear Regulatory Commission (NRC) Safety Goals (NRC, 1986). Again, the actual risk measures calculated will depend on the PRA Scope (Chapter 5).

The figure also indicates the importance of applying the principles of quality assurance in this task and all other task activities. Guidance for developing a quality assurance program is described in Chapter 4.

Finally, the output of this task goes directly to the Documentation task (Chapter 3).

16.2 Task Activities

16.2.1 Consequence Analysis

The consequences of an accidental release of radioactivity from a nuclear power plant to the surrounding environment can be expressed in several ways: impact on human health, impact on the environment, and impact on the economy. The consequence measures of most interest to a Level 3 PRA focus on the impact to human health. They should include:

- number of early fatalities,
- number of early injuries,
- number of latent cancer fatalities,
- population dose (person-rem or person-sievert) out to various distances from the plant,
- individual early fatality risk defined in the early fatality QHO, i.e., the risk of early fatality for the average individual within 1 mile from the plant, and
- individual latent cancer fatality risk defined in the latent cancer QHO, i.e., the risk of latent cancer fatality for the average individual within 10 miles of the plant.

The consequence measures that focus on impacts to the environment include:

- land contamination
- surface water body (e.g., lakes, rivers, etc.) contamination.

Groundwater contamination has yet to be included in a Level 3 analyses, although it may be important to consider it in certain specific cases.

The economic impacts are mainly estimated in terms of the costs of countermeasures taken to protect the population in the vicinity of the plant. These costs can include:

- short-term costs incurred in the evacuation and relocation of people during the emergency phase following the accident and in the destruction of contaminated food, and
- long-term costs of interdicting contaminated farmland and residential/urban property which cannot be decontaminated in a cost-effective manner, i.e., where the cost of decontamination is greater than the value of the property.

The costs of medical treatment to potential accident victims are not generally estimated in a Level 3 analysis, although approaches do exist for incorporating these costs (Mubayi et al., 1995) if required by the application.

The results of the calculations for each consequence measure are usually reported as a complementary cumulative distribution function. They can also be reported in terms of a distribution--for example, ones that show the 5th percentile, the 95th percentile, the median, and the mean.

16.2.1.1 Probabilistic Consequence Codes

A probabilistic consequence assessment (PCA) code is needed to perform the Level 3 analysis. Such codes normally take as input the characteristics of the release or source term provided by the Level 2 analysis. These characteristics typically include for each specified source term: the release fractions of the core inventory of key radionuclides, the timing and duration of the release, the height of the release (i.e., whether the release is elevated or ground level), and the energy of the release. PCA codes incorporate algorithms for performing weather sampling on the plume transport in order to obtain a distribution of the concentrations and dosimetry which reflect the uncertainty and/or variability due

to weather. The codes also model various protective action countermeasures to permit a more realistic calculation of doses and health effects and to assess the efficacy of these different actions in reducing consequences.

Several PCA codes are currently in use for calculating the consequences of postulated radiological releases. The NRC supports the use of the MACCS (Jow et al., 1990 and Chanin et al., 1993) and MACCS2 (Chanin and Young, 1997) PCA codes for carrying out nuclear power plant Level 3 PRA analyses. A number of countries in Europe support the use of the COSYMA (KfK and NRPB, 1991 and Jones et al., 1996) PCA code for their Level 3 analyses.

PCA codes require a substantial amount of information on the local meteorology, demography, land use, crops grown in various seasons, foods consumed, and property values. For example, the input file for the MACCS code requires the following information:

- Meteorology - one year of hourly data on: windspeed and direction, atmospheric stability class, precipitation rate, probability of precipitation occurring at specified distances from the plant site, and height of the atmospheric inversion layer.
- Demography - population distribution around the plant on a polar grid defined by 16 angular sectors and user-specified annular radial sectors, usually a finer grid close to the plant and one that becomes progressively coarser at greater distances.
- Land Use - fraction which is land, land which is agricultural, major crops, and growing season.
- Economic Data - value of farmland, value of nonfarm property, and annual farm sales.

The MACCS User Manual (Chanin et al., 1990) and the MACCS2 User Guide (Chanin and Young, 1997) may be consulted for a complete description of the site input data necessary.

In addition to site data, a PCA code should have provisions to model countermeasures to protect the public and provide a more realistic estimate of the doses and health effects following an accidental release. The MACCS code requires that the analyst make assumptions on the values of parameters related to the implementation of protective actions following an accident. The types of parameters involved in evaluating these actions include the following:

- delay time between the declaration of a general emergency and the initiation of an emergency response action, such as evacuation or sheltering; this delay time may be site specific,
- fraction of the offsite population which participates in the emergency response action,
- effective evacuation speed,
- degree of radiation shielding provided by the building stock in the area,
- projected dose limits for long-term relocation of the population from contaminated land, and
- projected ingestion dose limits used to interdict contaminated farmland.

The selected values assumed for the above (or similar) parameters need to be justified and documented since they have a significant impact on the consequence calculations.

In summary, the PCA code selected for the calculation of consequences should have the following capabilities:

- incorporate impact of weather variability on plume transport by performing stratified or Monte Carlo sampling on an annual set of relevant site meteorological data,
- allow for plume depletion due to dry and wet deposition mechanisms,
- allow for buoyancy rise of energetic releases,

- include all possible dose pathways, external and internal (such as cloudshine, groundshine, inhalation, resuspension inhalation, and ingestion) in the estimation of doses,
- employ validated health effects models based, for example, on (ICRP, 1991) or BEIR V (National Research Council, 1990) dose factors for converting radiation doses to early and latent health effects, and
- allow for the modeling of countermeasures to permit estimation of a more realistic impact of accidental releases.

The above-cited methods for estimating consequences are, in general, adequate for accidents caused by internal initiating events during both full power operation and shutdown conditions. However, for external initiating events, such as seismic events, certain changes may be needed. For example, the early warning systems and the road network may be disrupted so that initiation and execution of emergency response actions may not be possible. Hence, in addition to changing the potential source terms, a seismic event could also influence the ability of the close-in population to carry out an early evacuation. A Level 3 seismic PRA should, therefore, include consideration of the impacts of different levels of earthquake severity on the consequence assessment.

The final step in a Level 3 PRA is the integration of results from all previous analyses to compute the selected measures of risk. For a given consequence measure, risk is obtained as the sum over all postulated accidents of the product of the frequency and consequence of the accident. The methods for computing integrated risk are based on combining the results of all constituent analyses of the PRA, from initiating event and core damage frequencies calculated in the Level 1 analysis through the set of plant damage states and containment event trees and associated source term frequencies estimated in the Level 2 analysis to the conditional probabilities of the consequence measures evaluated in the Level 3 analysis. The methods used in the NUREG-1150 program (NRC, 1990) provide an acceptable method for obtaining the integrated risk.

16.2.1.2 Assumptions and Limitations

In most consequence codes, atmospheric transport of the released material is carried out assuming Gaussian plume dispersion. This assumption is generally valid for flat terrain to a distance of a few kilometers from the point of release but is inaccurate both in the immediate vicinity of the reactor building and at farther distances. For most PRA applications, however, the inaccuracies introduced by the assumption of Gaussian plumes are much smaller than the uncertainties due to other factors, such as the source term. In specific cases of plant location, such as, for example, a mountainous area or a valley, more detailed dispersion models that incorporate terrain effects may have to be considered. There are other physical parameters that influence downwind concentrations. Dry deposition velocity can vary over a wide range depending on the particle size distribution of the released material, the surface roughness of the terrain, and other factors. An assessment of these uncertainties focused on the factors which influence dispersion and deposition has been carried out recently (Harper et al., 1995). Earlier assessments of the assumptions and uncertainties in consequence modeling were reported in other PRA procedures guides (NRC, 1983).

Besides atmospheric transport, dispersion, and deposition of released material, there are several other assumptions, limitations, and uncertainties embodied in the parameters that impact consequence estimation. These include: models of the weathering and resuspension of material deposited on the ground, modeling of the ingestion pathway, i.e., the food chains, ground-crop-man and ground-crop-animal-dairy/meat-man, internal and external dosimetry, and the health effects model parameters. Other sources of uncertainty arise from the assumed values of parameters that determine the effectiveness of emergency response, such as the shielding provided by the building stock in the area where people are assumed to shelter, the speed of evacuation, etc. Comparison of the results of different consequence codes, which embody different approaches and values of these parameters, on a standard problem are contained

in a study sponsored by the Organisation for Economic Co-operation and Development (OECD, 1994). An uncertainty analysis of the COSYMA code results using the expert elicitation method is currently being carried out (Jones et al., 1996).

16.2.1.3 Required Input Data

To operate the consequence code, generally the following data elements are required:

- reactor radionuclide inventory,
- accident source terms defined by the release fractions of important radionuclide groups, the timing and duration of the release, and the energy and height of the release,
- hourly meteorological data at the site as recommended, for example, in Regulatory Guide 1.23 (NRC, 1986), collected over one or, preferably, more years and processed into a form usable by the chosen code,
- site population data from census or other reliable sources and processed in conformity with the requirements of the code, i.e., to provide population information for each areal element on the grid used in the code,
- site economic and land use data, specifying the important crops in the area, value and extent of farm and nonfarm property,
- defining the emergency response countermeasures, including the possible time delay in initiating response after declaration of warning and the likely participation in the response by the offsite population.

16.2.2 Computation of Risk

The final step in a Level 3 PRA is the integration of results from all previous analyses to compute individual measures of risk. The severe accident progression and the radionuclide source term analyses conducted in the Level 2 portion of the PRA, as well as the consequence analysis conducted in the Level 3 portion of the PRA, are performed on a conditional basis. That is, the evaluations of alternative severe accident progressions, resulting source terms, and consequences are performed without regard to the absolute or relative frequency of the postulated accidents. The final computation of risk is the process by which each of these portions of the accident analysis are linked together in a self-consistent and statistically rigorous manner.

The metric for judging the rigor of the process is the ability to demonstrate traceability from a specific accident sequence through the relative likelihood of alternative severe accident progressions and measures of attendant containment performance (i.e., early versus late failure) and ultimately to the distribution of radionuclide source terms and accident consequences. This traceability is evident in both directions (i.e., from an accident sequence to a distribution of consequences) and from a specific level of accident consequences back to the radionuclide source terms, containment performance measures, or accident sequences that contribute to that consequence level.

16.2.3 Additional Guidance

An important attribute by which the rigor of the process is likely to be judged is the ability to demonstrate traceability from a specific accident sequence through the relative likelihood of alternative severe accident progressions and measures of associated containment performance (i.e., early versus late failure) and ultimately to the distribution of fission product source terms and consequences. This traceability should be demonstrable in both directions, i.e., from the accident sequence to a distribution of consequences and from a specific level of accident consequences back to the fission product source terms, containment performance measures, or accident sequences that contribute to that consequence level. Guidance provided in Documentation (Chapter 3) and in conducting a quality PRA (Chapter 4) are crucial in assuring traceability of the PRA results.

16.3 Products

Documentation of the analyses performed to estimate the consequences associated with the

accidental release of radioactivity to the environment should contain sufficient information to allow an independent analyst to reproduce the results. At a minimum, the following information should be documented for the Level 3 analysis:

- identification of the consequence code and the version used to carry out the analysis,
- a description of the site-specific data and assumptions used in the input to the code,
- specifications of the source terms used to run the code, and
- discussion and definition of the emergency response parameters,
- a description of the computational process used to integrate the entire PRA model (Level 1 - Level 3),
- a summary of all calculated results including frequency distributions for each risk measure.

16.4 References

Chanin, D.I., and M. L. Young, "Code Manual for MACCS2: Volume 1, User's Guide," SAND97-0594, Sandia National Laboratories, March 1997.

Chanin, D.I., et al., "MACCS Version 1.5.11.1: A Maintenance Release of the Code," NUREG/CR-6059, Sandia National Laboratories, October 1993.

Chanin, D.I., et al., "MELCOR Accident Consequence Code System (MACCS), Volume 1, User's Guide," NUREG/CR-4691, Sandia National Laboratories, February 1990.

Harper, F. T., et al., "Probabilistic Accident Consequence Uncertainty Analysis, Dispersion, and Deposition Uncertainty Assessment," NUREG/CR-6244, Sandia National Laboratories, 1995.

ICRP, "1990 Recommendations of the ICRP," Annals of the ICRP, Vol. 21, No. 1-3, ICRP Publication 60, International Commission on Radiological Protection, Pergamon Press, Oxford, England, 1991.

Jones, J. A., et al., "Uncertainty Analysis on COSYMA," Proceedings of the Combined 3rd COSYMA Users Group and 2nd International MACCS Users Group Meeting, Portoroz, Slovenia, 41228-NUC 96-9238, KEMA, Arnhem, the Netherlands, September 16-19, 1996.

Jow, H. N., et al., "MELCOR Accident Consequence Code System (MACCS), Volume II, Model Description," NUREG/CR-4691, Sandia National Laboratories, February 1990.

KfK and NRPB, "COSYMA - A New Program Package for Accident Consequence Assessment," CEC Brussels, EUR 13028, Kernforschungszentrum (Karlsruhe) and National Radiological Protection Board, 1991.

Mubayi, V., et al., "Cost-Benefit Considerations in Regulatory Analysis," NUREG/CR-6395, Brookhaven National Laboratory, 1995.

National Research Council, "Health Effects of Exposure to Low Levels of Ionizing Radiation," BEIR V, Washington, DC, 1990.

NRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, Vol. 1, Main Report, U.S. Nuclear Regulatory Commission, 1990.

NRC, "Safety Goals for the Operation of Nuclear Power Plants, Policy Statement," Federal Register, Vol. 51, No. 149, U.S. Nuclear Regulatory Commission, August 4, 1986.

NRC, "Onsite Meteorological Programs," Regulatory Guide 1.23, U.S. Nuclear Regulatory Commission, April 1986.

NRC, "PRA Procedures Guide - A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, Vol. 2, U.S. Nuclear Regulatory Commission, 1983.

OECD, "Probabilistic Accident Consequence Assessment Codes, Second International Comparison", Organisation for Economic Co-operation and Development, Nuclear Energy Agency, Paris, France, 1994.

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

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG/CR-6572,Vol.3 Part 1
BNL-NUREG-52534

2. TITLE AND SUBTITLE

Severe Accident Risks for VVER Reactors:
The Kalinin PRA Program

Volume 3: Procedure Guides

3. DATE REPORT PUBLISHED

MONTH	YEAR
September	1999

4. FIN OR GRANT NUMBER

R9608

5. AUTHOR(S)

6. TYPE OF REPORT

Technical

7. PERIOD COVERED *(Inclusive Dates)*

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

Brookhaven National Laboratory
Upton, NY 11973-5000

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

Division of Risk Analysis and Applications
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES

11. ABSTRACT *(200 words or less)*

In order to facilitate the probabilistic risk assessment (PRA) of a VVER-1000 nuclear power plant, a set of procedure guides has been written. These procedure guides, along with training supplied by experts and supplementary material from the literature, were used to advance the PRA carried out for the Kalinin Nuclear Power Station in the Russian Federation. Although written for a specific project, these guides have general applicability. For a Level 1 PRA (determination of core damage frequency for different scenarios), the guides are written for all of the technical tasks involved for internal events, including internal fires and floods and seismic events. Guides are also provided for a Level 2 PRA (probabilistic accident progression and source term analysis) and a Level 3 PRA (consequence analysis and integrated risk assessment). In addition, introductory material is provided to explain the rationale and approach for a PRA. Procedure guides are also provided on the quality assurance and documentation requirements.

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

Probabilistic Risk Assessment, Procedure Guide, Soviet-Designed Reactors, VVER-1000, Kalinin Nuclear Power Station.

13. AVAILABILITY STATEMENT

unlimited

14. SECURITY CLASSIFICATION

(This Page)
unclassified

(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE

Federal Recycling Program

NUREG/CR-6572, Vol. 3 Part 1
September 1999