NUREG/CR-6572, Rev. 1
BNL-NUREG-52534-R1

Kalinin VVER-1000 Nuclear Power Station Unit 1 PRA

Procedure Guides for a Probabilistic Risk Assessment

English Version

Brookhaven National Laboratory

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555-0001

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment 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

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

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 Technical 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
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

NUREG/CR-6572, Rev. 1
BNL-NUREG-52534-R1

Kalinin VVER-1000 Nuclear Power Station Unit 1 PRA

Procedure Guides for a Probabilistic Risk Assessment

English Version

Manuscript Completed: May 2005
Date Published: December 2005

Sponsored by the Joint Cooperative Program Between the Governments of the United States and Russia

The BETA Project

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 R2001

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. Guides are procedures for all the technical tasks of a Level 1 (determination of core damage frequency for different accident scenarios), Level 2 (probabilistic accident progression and source term analysis), and Level 3 (consequence analysis and integrated risk assessment) PRA. In addition, introductory material is provided to explain the rationale and approach for a PRA. Procedure guides are also provided on the documentation requirements.

FOREWORD

During the Lisbon Conference on Assistance to the Nuclear Safety Initiative, held in May 1992, participants agreed that efforts should be undertaken to improve the safety of nuclear power plants that were designed and built by the former Soviet Union. That agreement led to a collaborative probabilistic risk assessment (PRA) of the Kalinin Nuclear Power Station (KNPS), Unit 1, in the Russian Federation. The KNPS Unit 1 PRA was intended to demonstrate the benefits obtained from application of risk technology towards understanding and improving reactor safety and, thereby, helping to build a risk-informed framework to help address reactor safety issues in regulations.

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 (Gosatomnadzor, or GAN) work together to begin applying PRA technology to Soviet-designed plants.[1] On the basis of that request, in 1995, the NRC and GAN agreed to work together to perform a PRA of a VVER-1000 PWR reactor. Under that agreement, the NRC provided financial support for the PRA with funds from AID and technical support primarily from Brookhaven National Laboratory and its subcontractors. KNPS Unit 1 was chosen for the PRA, and the effort was performed under the direction of GAN with the assistance of KNPS personnel and the following four other Russian organizations:

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

One of the overriding accomplishments of the project has been technology transfer. In NRC-sponsored workshops held in Washington, DC, and Moscow from October 1995 through November 2003, training was provided in all facets of PRA practice. In addition, the Russian participants developed expertise using current-generation NRC-developed computer codes, MELCOR, SAPHIRE and MACCS. Towards the completion of the PRA, senior members of the Kalinin project team began the development of risk-informed, Russian nuclear regulatory guidelines. These guidelines foster the application of risk assessment concepts to promote a better understanding of risk contributors. Efforts such as this have benefited from the expertise obtained, in part, from the training, experience, and insights gained from participation in the KNPS Unit 1 PRA project.

The documentation of the Kalinin PRA comprises two companion NUREG-series reports:

- NUREG/CR-6572, Revision 1, "Kalinin VVER-1000 Nuclear Power Station Unit 1 PRA: Procedure Guides for a Probabilistic Risk Assessment," was prepared by Brookhaven National Laboratory and the NRC staff. It contains guidance for conducting the Level 1, 2, and 3 PRAs for KNPS with primary focus on internal events. It may also serve as a guide for future PRAs in support of other nuclear power plants.

---

[1]As a result of a governmental decree in May 2004, GAN was subsumed into a new organization, known as the Federal Environmental, Industrial and Nuclear Supervision Service of Russia (Rostechnadzor).

- NUREG/IA-0212, "Kalinin VVER-1000 Nuclear Power Station Unit 1 PRA: Volumes 1 and 2," was written by the Russian team and, by agreement, includes both a non-proprietary and proprietary volume. The non-proprietary volume, Volume 1, "Executive Summary Report," discusses the project objectives, summarizes how the project was carried out, and presents a general summary of the PRA results. The proprietary volume, Volume 2, contains three parts. Part 1, "Main Report: Level 1 PRA, Internal Initiators," discusses the Level 1 portion of the PRA; Part 2, "Main Report: Level 2 PRA, Internal Initiators," discusses the Level 2 portion; and Part 3, "Main Report: Other Events Analysis," discusses preliminary analyses of fire, internal flooding, and seismic events, which may form the basis for additional risk assessment work at some future time.

Carl J. Paperiello

Carl J. Paperiello, Director
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(Continued)

Page

TABLE OF CONTENTS
(Continued)

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

The following organizations and individuals collaborated in performing the PRA for the Kalinin NPS, Unit 1:

U.S. Nuclear Regulatory Commission (NRC)

Charles Ader
Mark Cunningham
Mary Drouin
Thomas King
John Lane
Scott Newberry
Themis Speis
Andrew Szukiewicz

NRC Contractors

Mohammed Ali Azarm, Brookhaven National Laboratory (BNL)
Dennis Bley, Buttonwood Consulting Inc.
Tsong-Lun Chu, BNL
David Diamond, BNL
Ted Ginsberg, BNL
David Johnson, PLG Inc.
John Lehner, BNL
Mark Leonard, Dycoda
Hossein Nourbakhsh, BNL
Robert Kennedy, RPK Structural Mechanics Consulting
Robert Campbell, EQE International Inc.
Yang Park, BNL
Trevor Pratt, BNL
Jimin Xu, BNL

Federal Nuclear and Radiation Safety Authority of the Russian Federation (GAN), now the Federal Environmental, Industrial and Nuclear Supervision Service of Russia (Rostechnadzor)

Mikhail Mirochnitchenko
Alexandr Gutsalov
Alexandr Matveev

Science and Engineering Center for Nuclear and Radiation Safety

Irina Andreeva
Tatiana Berg
Valentina Bredova
Boris Gordon,
Irina Ioudina
Artour Lioubarski
Dmitri Noskov
Gennadi Samokhin
Eugene Shubeiko
Vyacheslav Soldatov
Sergei Volkovitskiy
Elena Zhukova

Kalinin Nuclear Power Station

Grigori Aleshin
Oleg Bogatov
Eugene Mironenko
Maxim Robotaev

Experimental and Design Office "Gidropress"

Viatcheslav Kudriavtsev
Valeri Siriapin
Vladimir Shein

Nizhny Novgorod Project Institute "Atomenergoprojekt"

Ludmila Eltsova
Vladimir Kats
Svetlana Petrunina
Valeri Senoedov
Alexander Yashkin

Rosenergoatom Consortium

Vladimir Khlebtsevich

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

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.[2] 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.

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

The scope of this guide is a full-scope PRA. There are a number of major components that comprise the scope of a PRA as illustrated in Figure 1.1.

1. It is necessary to identify all potential risks and decide on how many of these will be included in the PRA.

2. It is also necessary to determine the extent of the "population" exposed to the risks (e.g., health effects to the plant personnel or the surrounding population) and the "population" to be considered in the PRA.

3. 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.

4. 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.

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

[2] 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.

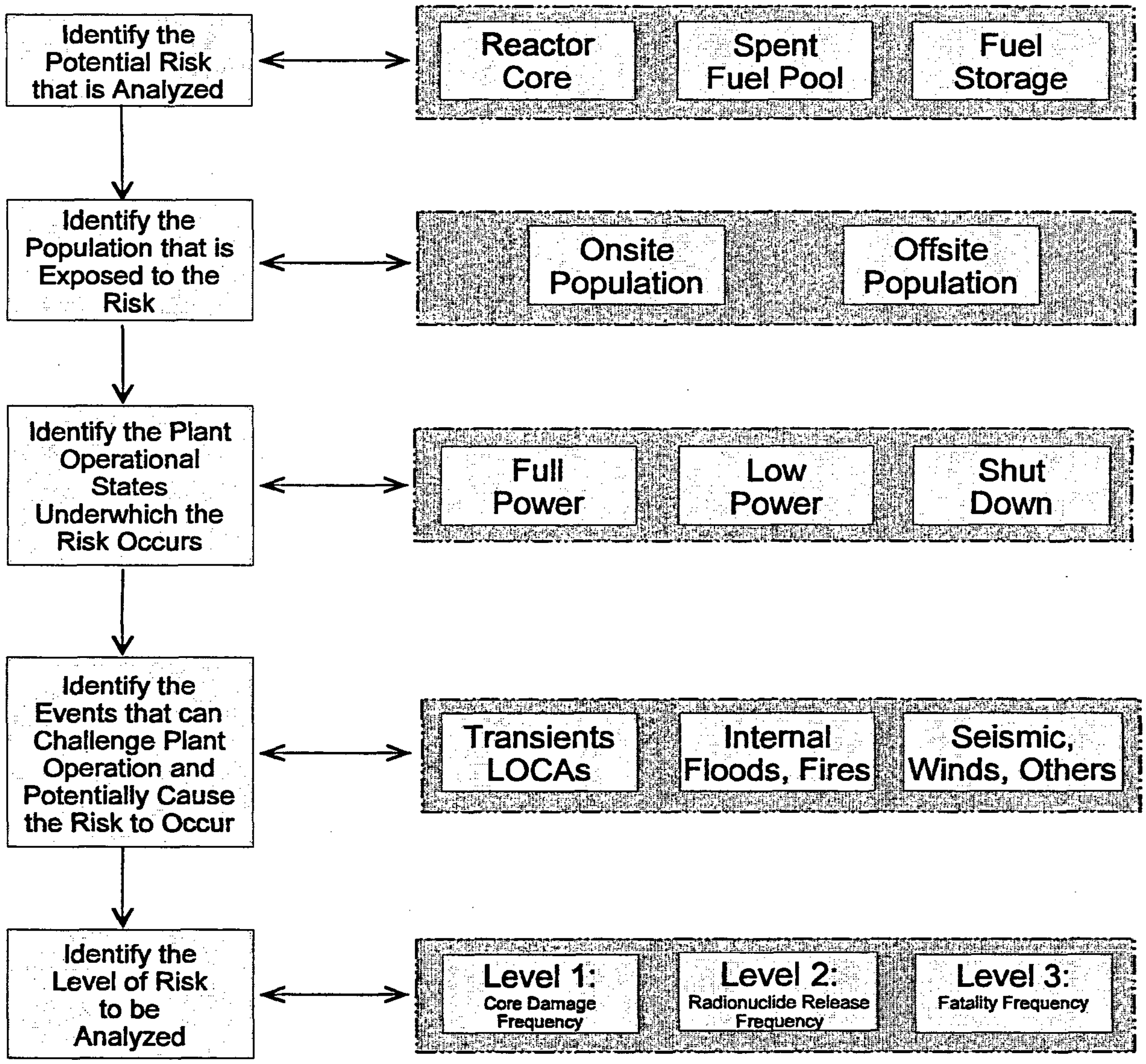

Figure 1.1 The six components comprising a PRA

- 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 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

PRA - Guides

It was assumed that the team carrying out the PRA would be familiar with the guides developed by the International Atomic Energy Agency (IAEA,1992 and IAEA,1995) for carrying out Level 1 and Level 2 PRAs for internal events. The IAEA documents represent internationally acceptable approaches. 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), NRC (1996) 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.

PRA - Assumptions and Limitations

The following assumptions and limitations are generally found in a PRA; regardless of its scope or analytical approach:

- 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.
- 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 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 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.

2. APPROACH

2.1 Scope of a PRA

The scope and quality of a PRA are key in determining the role PRA results can have in the decision-making regulatory activity. This section relies heavily on work reported in SECY-00-0162 (NRC, 2000). The scope of a PRA is defined by the following characteristics:

1. Degree of coverage of the potential hazards
2. Degree of coverage of the population exposed to the hazard
3. Degree of coverage of plant operating states (POSs) that define the plant's operating mode of concern: from full-power, to low-power, to shutdown modes of operation.
4. Degree of coverage of initiating events, either internal or external to the plant boundary, that cause off-normal conditions.
5. Level of characterization of risk:
   a. Level 1 PRA that estimates the CDF (given an event that challenges plant operation occurs).
   b. Level 2 PRA that estimates the containment failure and radionuclide release frequencies (given a core damage state occurs).
   c. Level 3 PRA that estimates the offsite consequences from a release, e.g., early and latent cancer fatalities (given a radionuclide release occurs).

NRC Regulatory Guide 1.200 (NRC, 2004) describes an approach for determining that the quality of a PRA is adequate and so provide confidence in its results. This guidance is consistent with existing NRC PRA policy, and it reflects on-going work by U.S. standard-setting and nuclear industry organizations.

Hazards cover a wide range of events that could potentially cause damage and health effects. For the purpose of performing a PRA of a NPP the hazards considered are those materials located on the site that if released could potentially contaminate the environment and cause health effects to the on-site and off-site population. Generally hazards resulting from the release of radionuclides are considered. There are three possible sources of radionuclide release:

- Reactor Core
- Spent Fuel Pool
- Fuel Storage

The population that could be exposed to the hazard include on-site workers and members of the population in the vicinity of the plant. The 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.

Plant operating states (POSs) are used to subdivide the plant operating cycle into unique states such that the plant response can be assumed to be the same for all subsequent accident initiating events. Operational characteristics (such as reactor power level; in-vessel temperature, pressure, and coolant level; equipment operability; and changes in decay heat load or plant conditions that allow new success criteria) are examined to identify those important to defining plant operational states. The important characteristics are used to define the states and the fraction of time spent in each state is estimated using plant specific information. The risk perspective should be based on the total risk connected with the operation of the reactor which includes not only full power operation, but low power and shutdown conditions. Therefore, to gain the maximum benefit from a PRA, the model should address all modes of operation.

Initiating events are events that have the ability to challenge the condition of the plant. These events include failure of equipment from either "internal plant causes" such as hardware faults, operator actions, floods or fires, or "external plant causes" such as seismic or high winds.

The risk perspective should be based on the total risk connected with the operation of the reactor which includes events from both internal and external sources. Therefore, to gain the maximum benefit from a PRA, the model should address both internal and external initiating events.

The risk characterization used in risk-informed applications are the core damage frequency (CDF) and health effects (to the surrounding population); therefore, to provide the risk perspective for use in decision-making, a Level 1, 2, and 3 PRA is required.

2.2 Scope of the Guides

An essential part of the PRA process is having confidence in the PRA results such that they can be used in decision making. An independent peer review of the PRA can provide confidence in the results. Therefore, the scope of the PRA guides includes guidance for both performing the technical work, and performing a peer review of the technical work.

2.2.1 Technical Guidance

As noted above, the scope of a PRA includes:

- the degree of coverage of
  - potential hazards
  - population impacted
  - plant operating states
  - initiating events
- level of risk characterization.

The first major item above defines the scope of the PRA, while the second major item defines the analytical levels to be performed for the given scope. For this project, the PRA scope is limited to the following:

- hazards including accidents that involve the reactor core
- offsite population
- accidents occurring while the plant is operating at full power
- initiating events internal and external to the plant

The procedure guides contained in this report address this scope for all three analytical levels.

The technical elements for each analytical level are listed in the Table 2-1 and briefly described below.

Plant Familiarization and Documentation are not separate elements in of themselves but rather impact all of the technical elements as noted in Table 2-1. As Plant Familiarization is required for all of the technical elements, it is discussed first. Documentation is discussed last because all of the technical elements provide input this element.

The guidelines for performing the technical elements for the above defined scope are provided in Chapter 3.

<u>**Plant Familiarization**</u> —

Before the technical analysis can begin, it is imperative that the analysis team becomes familiar with all aspects of the plant. The quality of information gathered in this task and the manner in which it is managed is critical to the success of the entire analysis effort. This information gathering process provides assurance that the possible core damage accident sequences are correctly defined and realistically describe the possible plant responses.

As this task provides the basic plant information needed to perform the analytical work 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.

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 a configuration freeze date, i.e., the date after which plant changes will not be included in the analysis, should be established.

Table 2-1 Technical elements of a PRA

Scope/Level of Analysis	Technical Elements (Note)	
Risk Characterization (full power, internal events – transients and loss of coolant accidents)		
Level 1	• Initiating Event Analysis • Success Criteria Analysis • Accident Sequence Analysis • Systems Analysis	• Parameter Estimation Analysis • Human Reliability Analysis • Quantification Analysis • Interpretation of Results
Level 2	• Plant Damage State Analysis • Accident Progression Analysis • Source Term Analysis	• Quantification • Interpretation of Results
Level 3	• Data Collection • Source Term Reduction	• Consequence Calculation • Risk Integration
Initiating Events (Other Events)		
Internal Flood	• Identification Analysis • Evaluation Analysis	• Quantification Analysis
Internal Fire	• Screening Analysis • Fire Initiation Analysis	• Fire Damage Analysis • Plant Response Analysis
External Events	• Screening/Bounding Analysis • Events Analysis	• Fragility Analysis • Level 1 Model Modification

Risk Characterization —

Level 1 PRA

The following provides a description of each of the Level 1 technical elements.

Initiating event analysis identifies and characterizes those random internal events that both challenge normal plant operation during power or shutdown conditions and require successful mitigation by plant equipment and personnel to prevent core damage from occurring. Events that have occurred at the plant and those that have a reasonable probability of occurring are identified and characterized. An understanding of the nature of the events is performed such that a grouping of the events into event classes, with the classes defined by similarity of system and plant responses (based on the success criteria), may be performed to manage the large number of potential events that can challenge the plant.

Success criteria analysis determines the minimum requirements for each function (and ultimately the systems used to perform the functions) needed to prevent core damage (or to mitigate a release) given an initiating event occurs. The requirements defining the success criteria are based on acceptable engineering analyses that represent the design and operation of the plant under consideration. The criteria needed for a function to be successful is dependent on the initiator and the conditions created by the initiator. The code(s) used to perform the analyses for developing the success criteria are validated and verified for both technical integrity and suitability to assess plant conditions for the reactor pressure, temperature and flow range of interest, and accurately analyze the phenomena of interest. Calculations are performed by personnel qualified to perform the types of analyses of interest and are well trained in the use of the code(s).

Accident sequence analysis models, chronologically, the different possible progression of events (i.e., accident sequences) that can occur from the start of the initiating event to either successful mitigation or to core damage. The accident sequences account for those systems and operator actions that are used (and available) to mitigate the initiator based on the defined success criteria and plant operating procedures (e.g., plant emergency and abnormal operating procedures and as practiced in simulator exercises). The availability of a system includes consideration of the functional, phenomenological and operational dependencies and interfaces between and among the different systems and operator actions during the course of the accident progression.

Systems analysis identifies the different combinations of failures that can preclude the ability of the system to perform its function as defined by the success criteria. The model representing the various failure combinations includes, from an as-built and as-operated perspective, the system hardware and instrumentation (and their associated failure modes) and the human failure events that would prevent the system from performing its defined function. The basic events representing equipment and human failures are developed in sufficient detail in the model to account for dependencies between and among the different systems, and to distinguish the specific equipment or human event (and its failure mechanism) that has a major impact on the system's ability to perform its function.

Parameter estimation analysis quantifies the frequencies of the identified initiators and quantifies the equipment failure probabilities and equipment unavailabilities of the modeled systems. The estimation process includes a mechanism for addressing uncertainties, has the ability to combine different sources of data in a coherent manner, and represents the actual operating history and experience of the plant and applicable generic experience as applicable.

Human reliability analysis identifies and quantifies the human failure events that can negatively impact normal or emergency plant operations. The human failure events associated with normal plant operation include those events that leave the system (as defined by the success criteria) in an unrevealed, unavailable state. The human failure events associated with emergency plant operation include those events that, if not performed, do not allow the needed system to function. Quantification of the probabilities of these human failure events are based on plant and accident specific conditions, where applicable, including any dependencies among actions and conditions.

Quantification analysis provides an estimation of the CDF given the design, operation and maintenance of the plant. This CDF is based on the summation of the estimated CDF from each initiator class. If truncation of accident sequences and cutsets is applied, truncation limits are set so that the overall model results are not impacted significantly and that important accident sequences are not eliminated. Therefore, the truncation limit can vary for each accident sequence. Consequently, the truncation value is selected so that the accident sequence CDF before and after truncation only differs by less than one significant figure.

Interpretation of results entails examining and understanding the results of the PRA and identifying the important contributors sorted by initiating events, accident sequences, equipment failures and human errors. Methods such as importance measure calculations (e.g., Fussel-Vesely, risk achievement, risk reduction, and Birnbaum) are used to identify the contributions of various events to the model estimation of core damage frequency for both individual sequences and the model as a total. Sources of uncertainty are identified and their impact on the results analyzed. The sensitivity of the model results to model boundary conditions and other key assumptions is evaluated using sensitivity analyses to look at key assumptions both individually or in logical combinations. The combinations analyzed are chosen to fully account for interactions among the variables.

Level 2 PRA

The following provides a description of each of the Level 2 technical elements.

Plant damage state analysis groups similar core damage scenarios resulting from the full spectrum of core damage accidents identified in the Level 1 analysis to allow a practical assessment of the severe accident progression and containment response. The plant damage state analysis defines the attributes of the core damage scenarios that represent important boundary conditions to the assessment of severe accidents progression and containment response that ultimately affect the resulting source term. The attributes address the dependencies between the containment systems modeled in the Level 2 analysis with the core damage accident sequence models to fully account for mutual dependencies. Core damage scenarios with similar attributes are grouped together to allow for efficient evaluation of the Level 2 response.

Severe accident progression analysis models the different series of events that challenge containment integrity for the core damage scenarios represented in the plant damage states. The accident progressions account for interactions among severe accident phenomena and system and human responses to identify credible containment failure modes including failure to isolate the containment. The timing of major accident events and the subsequent loadings produced on the containment are evaluated against the capacity of the containment to withstand the potential challenges. The containment performance during the severe accident is characterized by the timing (e.g., early versus late), size (e.g., catastrophic versus bypass), and location of any containment failures. The code(s) used to perform the analysis are validated and verified for both technical integrity and suitability. Calculations are performed by personnel qualified to perform the types of analyses of interest and well trained in the use of the code(s).

Source term analysis characterizes the radiological release to the environment resulting from each severe accident sequence leading to containment failure or bypass. The characterization includes the time, elevation, and energy of the release and the amount, form, and size of the radioactive material that is released to the environment.

Quantification integrates the accident progression models and source term evaluation to provide estimates of the frequency of radionuclide releases that could be expected following the identified core damage accidents. This quantitative evaluation reflects the different magnitudes and timing of radionuclide releases.

Interpretation of results entails examining results from importance measure calculations (e.g., Fussel-Vesely, risk achievement, risk reduction, and Birnbaum) to identify the contributions of various events to the model estimation of risk for both individual sequences and the model as a total. Sources of uncertainty are identified and their impact o the results analyzed. The sensitivity of the model results to model boundary conditions and other key assumptions is evaluated using sensitivity analyses to look at key assumptions both individually or in logical combinations. The combinations analyzed are chosen to fully account for interactions among the variables.

Level 3 PRA

The following provides a description of each of the Level 3 technical elements.

Data Collection is a compilation of the demographic and weather-related data needed to predict how the radionuclides will be dispersed to the environment. 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).

Source Term Reduction groups severe accident progressions resulting from the full spectrum of severe accidents into a smaller number of representative "release categories" to allow a practical assessment of the offsite consequences. The reduction process identifies the attributes that represent important boundary conditions that ultimately affect the offsite consequences. Accident progressions with these similar attributes are grouped together to allow for efficient evaluation of the Level 3 analysis.

Consequence Calculations provide a conditional estimation of the early and latent fatalities and the extent of land contamination that would be expected following severe accidents. This quantification does not reflect the actual risk associated with operating the plant (this is estimated in the risk integration task below), but deterministically calculates for each of the representative "release categories" the dispersal of the radioactive plume in the environment, the dose (and associated health effects) to the population and contamination of the surrounding land.

Risk Integration combines the results from all previous analyses (i.e., CDF, release frequency and conditional fatalities) 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.

<u>Other Events</u> —

The following provides a description of each of the Other Events technical elements. In addressing the above elements, because of the nature and impact of internal flood and fire and external hazards, their attributes need to be discussed separately. This is because flood, fire and external hazards analyses have the ability to cause initiating events but also have the capability to impact the availability of mitigating systems. Therefore, in developing the PRA model, the impact of flood, fire and external hazards needs to be considered in each of the above technical elements. A summary of the desired attributes of an acceptable internal flood and fire and external hazards analyses is provided below.

Internal Floods

Identification analysis identifies those plant areas where flooding could pose significant risk. Flooding areas are defined on the basis of physical barriers, mitigation features, and propagation pathways. For each flooding area, flood sources due to equipment (e.g., piping, valves, pumps), internal (e.g., tanks) and external (e.g., rivers) water sources are identified along with the affected SSCs. Flooding mechanisms are examined which include failure modes of components, human induced mechanisms, and other water releasing events. Flooding types (e.g., leak, rupture, spray) and flood sizes are determined. Plant walkdowns are performed to verify the accuracy of the information.

Evaluation analysis identifies the potential flooding scenarios for each flood source by identifying flood propagation paths of water from the flood source to its accumulation point (e.g., pipe and cable penetrations, doors, stairwells, failure of doors or walls). Plant design features or operator actions that have the ability to terminate the flood are identified. Credit given for flood isolation is justified. The susceptibility of each SSC in a flood area to flood-induced mechanisms is examined (e.g., submerge, spray, pipe whip, and jet impingement). Flood scenarios are developed by examining the potential for propagation and giving credit for flood mitigation. Flood scenarios can be eliminated on the basis of screening criteria. The screening criteria used are well defined and justified.

Quantification analysis provides an estimation of the CDF of the plant due to internal floods. Flooding induced initiating events that represent the design, operation and experience of the plant are identified and their frequencies quantified. The Level 1 models are modified and the internal flood accident sequences quantified: (1) modify accident sequence models to address flooding phenomena, (2) perform necessary calculations to determine success criteria for flooding mitigation, (3) perform parameter estimation analysis to include flooding as a failure mode, (4) perform human reliability analysis to account for PSFs due to flooding, and (5) quantify internal flood accident sequence CDF. Modification of the Level 1 models are performed consistent with the characteristics for Level 1 elements for transients and LOCAs. In addition, sources of uncertainty are identified and their impact o the results analyzed. The sensitivity of the model results to model boundary conditions and other key assumptions is evaluated using sensitivity analyses to look at key assumptions both individually or in logical combinations. The combinations analyzed are chosen to fully account for interactions among the variables.

Internal Fires

Screening analysis identifies fire areas where fires could pose a significant risk. Fire areas which are not risk significant can be "screened out" from further consideration in the PRA analysis. Both qualitative and quantitative screening criteria can be used. The former address whether an unsuppressed fire in the area poses a nuclear safety challenge; the latter are compared against a bounding assessment of the fire-induced core damage frequency for the area. The potential for fires involving multiple areas should be addressed. Assumptions used in the screening analysis should be verified through appropriate plant walkdowns. Key screening analysis assumptions and results, e.g., the area-specific conditional core damage probabilities (assuming fire-induced loss of all equipment in the area), should be documented.

Fire initiation analysis determines the frequency and physical characteristics of the detailed (within-area) fire scenarios analyzed for the unscreened fire areas. The analysis needs to identify a range of scenarios which will be used to represent all possible scenarios in the area. The possibility of seismically-induced fires should be considered. The scenario frequencies should reflect plant-specific experience, and should be quantified in a manner that is consistent with their use in the subsequent fire damage analysis (discussed below). The physical characterization of each scenario should also be in terms that will support the fire damage analysis (especially with respect to fire modeling).

Fire damage analysis determines the conditional probability that sets of potentially risk-significant components (including cables) will be damaged in a particular mode, given a specified fire scenario. The analysis needs to address components whose failure will cause an initiating event, affect the plant's ability to mitigate an initiating event, or affect potentially risk significant equipment (e.g., through suppression system actuation). Damage from heat, smoke, and exposure to suppressants should be considered. If fire models are used to predict fire-induced damage, compartment-specific features (e.g., ventilation, geometry) and target-specific features (e.g., cable location relative to the fire) should be addressed. The fire suppression analysis should account for the scenario-specific time required to detect, respond to, and extinguish the fire. The models and data used to analyze fire growth, fire suppression, and fire-induced component damage should be consistent with experience from actual nuclear power plant fire experience as well as experiments.

Plant response analysis involves the modification of appropriate plant transient and LOCA PRA models to determine the conditional core damage probability, given damage to the set(s) of components defined in the fire damage analysis. All potentially significant fire-induced initiating events, including such "special" events as loss of plant support systems, and interactions between multiple nuclear units during a fire event, should be addressed. The analysis should address the availability of non-fire affected equipment (including control) and any required manual actions. For fire scenarios involving control room abandonment, the analysis should address the circuit interactions raised in NUREG/CR-5088, including the possibility of fire-induced damage prior to transfer to the alternate shutdown panel(s). The human reliability analysis of operator actions should address fire effects on operators (e.g., heat, smoke, loss of lighting, effect on instrumentation) and fire-specific operational issues (e.g., fire response operating procedures, training on these procedures, potential complications in coordinating activities). In addition, sources of uncertainty are identified and their impact o the results analyzed. The sensitivity of the model results to model boundary conditions and other key assumptions is evaluated using sensitivity analyses to look at key assumptions both individually or in logical combinations. The combinations analyzed are chosen to fully account for interactions among the variables.

External Events

Screening and bounding analysis identifies external events other than earthquake that may challenge plant operations and require successful mitigation by plant equipment and personnel to prevent core damage from occurring. The term "screening out" is used here for the process whereby an external event is excluded from further consideration in the PRA analysis. There are two fundamental screening criteria embedded in the requirements here, as follows: An event can be screened out either (I) if it meets the certain design criteria, or (ii) if it can be shown using an analysis that the mean value of the design-basis hazard used in the plant design is less than 10-5/year, and that the conditional core-damage probability is less than 10-1, given the occurrence of the design-basis hazard. An external event that cannot be screened out using either of these criteria is subjected to the detailed-analysis.

Event Analysis characterizes non-screened external events and seismic events, generally, as frequencies of occurrence of different sizes of events (e.g., earthquakes with various peak ground accelerations, hurricanes with various maximum wind speeds) at the site. The external events are site specific and include both aleatory and epistemic uncertainties.

Fragility Analysis characterizes conditional probability of failure of important structures, components, and systems whose failure may lead to unacceptable damage to the plant (e.g., core damage) given occurrence of an external event. For important SSCs, the fragility analysis is realistic and plant-specific. The fragility analysis is based on extensive plant-walkdowns reflecting as-built, as-operated conditions.

Level 1 Model Modification assures that the system models include all important external-event caused initiating events that can lead to core damage or large early release. The system model includes external-event induced SSC failures, non-external-event induced failures (random failures), and human errors. The system analysis is well coordinated with the fragility analysis and is based on plant walkdowns. The results of the external event hazard analysis, fragility analysis, and system models are assembled to estimate frequencies of core damage and large early release. Uncertainties in each step are propagated through the process and displayed in the final results. The quantification process is capable of conducting necessary sensitivity analysis and to identify dominant sequences and contributors.

Documentation —

Traceability and defensibility provides the necessary information such that the results can easily be reproduced and justified. The sources of information used in the PRA are both referenced and retrievable. The methodology used to perform each aspect of the work is described either through documenting the actual process or through reference to existing methodology documents. Assumptions(1) made in performing the analyses are identified and documented along with their justification to the extent that the context of the assumption is understood. The results (e.g., products and outcomes) from the various analyses are documented.

2.2.2 Guidance for Peer Review Process

A peer review process can be used to identify weaknesses in the PRA and the importance of the weaknesses to the confidence in the PRA results. An acceptable peer review needs to be performed by qualified personnel, needs to be performed according to an established process that compares the PRA against desired characteristics and attributes, and needs to document the results including both strengths and weaknesses of the PRA.

The team qualifications determine the credibility and acceptability of the peer reviewers. The peer reviewers should not give any perception of a conflict of interest, therefore, they should be independent of the PRA and not have performed any technical work on the PRA. The members of the peer review team should have technical expertise in the PRA elements they review including experience in the specific methods that are utilized to perform the PRA elements. In addition, knowledge of the specific plant design and operation is essential. Finally, each member of the peer review team should be knowledgeable of the peer review process including the desired characteristics and attributes used to assess the acceptability of the PRA.

The peer review process includes a documented procedure to direct the team in evaluating the acceptability of a PRA. The review process should compare the PRA against the desired PRA characteristics and attributes, which are listed in Table 2-2 below. In addition, to reviewing the methods utilized in the PRA, the peer review also determines if the application of those methods were done correctly. The PRA models should be compared against the plant design and procedures to validate that they reflect the as-built and as-operated plant. Key assumptions should be reviewed to determine if they are appropriate and if they have a significant impact on the PRA results. The PRA results should be checked for fidelity with the model structure and also for consistency with the results from PRAs for similar plants. Finally, the peer review process should examine the procedures or guidelines in place for updating the PRA to reflect changes in plant design, operation, or experience.

Documentation provides the necessary information such that the peer review process and the findings are both traceable and defensible. A description of the qualifications of the peer review team members and the peer review process should be documented. The results of the peer review for each technical element and the PRA update process should be described including those areas where the PRA do not meet or exceed the desired characteristics and attributes used in the review process. This includes an assessment of the importance of any identified deficiencies on the PRA results and potential uses and how these deficiencies were addressed and resolved.

2.3 References

NRC, "Addressing PRA Quality in Risk-Informing Activities," SECY-00-0162, July 28, 2000.

NRC, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," Regulatory Guide 1.200, issued for trial use, February 2004.

Table 2-2 Summary of technical characteristics and attributes of a PRA

Element	Technical Characteristics and Attributes
Plant Familiarization	• identification of plant information sources to provide sufficient plant knowledge such that the PRA model represents the as-built and as-operated plant and reflects the actual operating history • design and operational understanding confirmed by actual plant walkdowns and interviews of operators
Level 1 PRA (internal events – transients and loss of coolant accidents (LOCAs))	
Initiating Event Analysis	• sufficiently detailed identification and characterization of initiators • grouping of individual events according to plant response and mitigating requirements • proper screening of any individual or grouped initiating events
Success Criteria Analysis	• based on best-estimate engineering analyses applicable to the actual plant design and operation • codes developed, validated, and verified in sufficient detail - analyze the phenomena of interest - be applicable in the pressure, temperature, and flow range of interest
Accident Sequence Development Analysis	• defined in terms of hardware, operator action, and timing requirements and desired end states (e.g., CD or PDSs) • includes necessary and sufficient equipment (safety and non-safety) reasonably expected to be used to mitigate initiators • includes functional, phenomenological, and operational dependencies and interfaces
Systems Analysis	models developed in sufficient detail to: • reflect the as built, as operated plant including how it has performed during the plant history • reflect the required success criteria for the systems to mitigate each identified accident sequence • capture impact of dependencies, including support systems and harsh environmental impacts • include both active and passive components and failure modes that impact the function of the system • include common cause failures, human errors, unavailability due to test and maintenance, etc.

Table 2-2 Summary of technical characteristics and attributes of a PRA (cont'd)

Element	Technical Characteristics and Attributes
Parameter Estimation Analysis	• estimation of parameters associated with initiating event, basic event probability models, recovery actions, and unavailability events that account for plant-specific and generic data • consistent with component boundaries • estimation includes a characterization of the uncertainty
Human Reliability Analysis	• identification and definition of the human failure events that would result in initiating events or pre- and post-accident human failure events that would impact the mitigation of initiating events • quantification of the associated human error probabilities taking into account scenario (where applicable) and plant-specific factors and including appropriate dependencies both pre- and post-accident
Quantification	• estimation of the CDF for modeled sequences that are not screened due to truncation, given as a mean value • estimation of the accident sequence CDFs for each initiating event group • truncation values set relative to the total plant CDF such that the frequency in not significantly impacted
Interpretation of Results	• identification of the key contributors to CDF: initiating events, accident sequences, equipment failures and human errors • identification of sources of uncertainty and their impact on the results • understanding of the impact of the key assumptions* on the CDF and the identification of the accident sequence and their contributors
Level 2 PRA	
Plant Damage State Analysis	• identification of the attributes of the core damage scenarios that influence severe accident progression, containment performance, and any subsequent radionuclide releases • grouping of core damage scenarios with similar attributes into plant damage states • carryover of relevant information from Level 1 to Level 2
Severe Accident Progression Analysis	• use of verified, validated codes by qualified trained users with an understanding of the code limitations and the means for addressing the limitations • assessment of the credible severe accident phenomena via a structured process • assessment of containment system performance including linkage with failure modes on non-containment systems • establishment of the capacity of the containment to withstand severe accident environments • assessment of accident progression timing, including timing of loss of containment failure integrity
Quantification	• estimation of the frequency of different containment failure modes and resulting radionuclide source terms

Table 2-2 Summary of technical characteristics and attributes of a PRA (cont'd)

Element	Technical Characteristics and Attributes
Source Term Analysis	• assessment of radionuclide releases including appreciation of timing, location, amount and form of release • grouping of radionuclide releases into smaller subset of representative source terms with emphasis on large early release (LER) and on large late release (LLR)
Interpretation of Results	• identification of the contributors to containment failure and resulting source terms • identification of sources of uncertainty and their impact on the results • understanding of the impact of the key assumptions* on Level 2 results
Level 3	
Data Collection	• data regarding local meteorology and terrain, site demographics, and local land use represent current, plant-specific condition.
Source Term Reduction	• source terms used to calculate offsite consequences preserve the full range of early (mechanistic) and late (stochastic) health effects that would result from actual Level 2 source terms.
Consequence Calculation	• variability in weather addressed as major uncertainty in consequences
Risk Integration	• integrates results of Level 1, 2 and 3 to compute various measures of risk. • each of the three PRA Levels are linked together in a self-consistent and statistically rigorous manner.
Internal Flood Analysis	
Identification Analysis	• sufficiently detailed identification and characterization of: - flood areas and SSCs located within each area - flood sources and flood mechanisms - the type of water release and capacity - the structures functioning as drains and sumps • verification of the information through plant walkdowns
Evaluation Analysis	• identification and evaluation of - flood propagation paths - flood mitigating plant design features and operator actions - the susceptibility of SSCs in each flood area to the different types of floods • elimination of flood scenarios uses well defined and justified screening criteria

Table 2-2 Summary of technical characteristics and attributes of a PRA (cont'd)

Element	Technical Characteristics and Attributes
Quantification	• identification of flooding induced initiating events on the basis of a structured and systematic process • estimation of flooding initiating event frequencies • estimation of CDF for chosen flood sequences • modification of the Level 1 models to account for flooding effects including uncertainties
Internal Fire Analysis	
Screening Analysis	• all potentially risk-significant fire areas are identified and addressed • all required mitigating components and their cables in each fire area are identified • screening criteria are defined and justified • necessary walkdowns are performed to confirm the screening decisions • screening process and results are documented • unscreened events areas are subjected to appropriate level of evaluations (including detailed fire PRA evaluations as described below) as needed
Fire Initiation Analysis	• all potentially significant fire scenarios in each unscreened area are addressed • fire scenario frequencies reflect plant-specific features • fire scenario physical characteristics are defined • bases are provided for screening fire initiators
Fire Damage Analysis	• damage to all potentially significant components is addressed; considers all potential component failure modes • all potentially significant damage mechanisms are identified and addressed; damage criteria are specified • analysis addresses scenario-specific factors affecting fire growth, suppression, and component damage • models and data are consistent with experience from actual fire experience as well as experiments • includes evaluation of propagation of fire and fire effects (e.g., smoke) between fire compartments
Plant Response Analysis	• all potentially significant fire-induced initiating events are addressed so that their bases are included in the model • includes fire scenario impacts on core damage mitigation and containment systems including fire-induced failures • analysis reflects plant-specific safe shutdown strategy • potential circuit interactions which can interfere with safe shutdown are addressed • human reliability analysis addresses effect of fire scenario-specific conditions on operator performance

Table 2-2 Summary of technical characteristics and attributes of a PRA (cont'd)

Element	Technical Characteristics and Attributes
Quantification	• estimation of fire CDF for chosen fire scenarios • identification of sources of uncertainty and their impact on the results • understanding of the impact of the key assumptions* on the CDF • all fire risk-significant sequences are traceable and reproducible
External Events Analysis	
Screening and Bounding Analysis	• credible external events (natural and man-made) that may affect the site are addressed • screening and bounding criteria are defined and results are documented • necessary walkdowns are performed • non-screened events are subjected to appropriate level of evaluations
Event Analysis	• the event analysis is site and plant-specific • the event analysis addresses uncertainties
Fragility Analysis	• fragility estimates are plant-specific for important SSCs • walkdowns are conducted to identify plant-unique conditions, failure modes, and as-built conditions.
Level 1 Model Modification	• important external event caused initiating events that can lead to core damage and large early release are included • external event related unique failures and failure modes are incorporated • equipment failures from other causes and human errors are included. When necessary, human error data is modified to reflect unique circumstances related to the external event under consideration • unique aspects of common causes, correlations, and dependencies are included • the systems model reflects as-built, as-operated plant conditions • the integration/quantification accounts for the uncertainties in each of the inputs (i.e., hazard, fragility, system modeling) and final quantitative results such as CDF and LERF • the integration/quantification accounts for all dependencies and correlations that affect the results
Documentation	
Traceability and defensibility	• The documentation is sufficient to facilitate independent peer reviews • The documentation describes all of the important interim and final results, insights, and important sources of uncertainties • Walkdown process and results are fully described

*Assumptions include those decisions and judgments that were made in the course of the analysis.

3. TECHNICAL ACTIVITIES

This chapter provides the guidance for the analytical tasks needed to perform the technical elements of the PRA for the scope defined in Chapter 2. This scope includes:

- hazards involving reactor core accidents
- offsite population
- accidents occurring while the plant is operating at full power
- initiating events internal and external to the plant

The guides contained in this chapter address this scope for all three analytical levels.

The technical elements for each analytical level are listed in Table 3-1 and their associated guides described below.

Plant Familiarization and documentation are not separate elements in of themselves but rather impact all of the technical elements as noted in Table 3-1. As plant familiarization is required for all of the technical elements it is discussed first. Documentation is discussed in Chapter 4.

Table 3-1 Technical elements of a PRA

Scope/Level of Analysis	Technical Elements (Note)	
Risk Characterization (full power, internal events – transients and loss of coolant accidents)		
Level 1	• Initiating Event Analysis • Success Criteria Analysis • Accident Sequence Analysis • Systems Analysis	• Parameter Estimation Analysis • Human Reliability Analysis • Quantification Analysis • Interpretation of Results
Level 2	• Plant Damage State Analysis • Accident Progression Analysis • Source Term Analysis	• Quantification • Interpretation of Results
Level 3	• Data Collection • Source Term Reduction	• Consequence Calculation • Risk Integration
Initiating Events (Other Events)		
Internal Flood	• Identification Analysis • Evaluation Analysis	• Quantification Analysis
Internal Fire	• Screening Analysis • Fire Initiation Analysis	• Fire Damage Analysis • Plant Response Analysis
External Events	• Screening/Bounding Analysis • Events Analysis	• Fragility Analysis • Level 1 Model Modification

3.1 Plant Familiarization

This section describes the Plant Familiarization Analysis task. Before the technical analysis can begin, it is imperative that the analysis team becomes familiar with all aspects of the plant. The quality of information gathered in this task and the manner in which it is managed is critical to the success of the entire analysis effort. This information gathering process provides assurance that the possible core damage accident sequences are correctly defined and realistically describe the possible plant responses.

3.1.1 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.

3.1.2 Products

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 products for this task are provided below:

- A 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 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.

3.1.3 Task Activities

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

The second task, 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 task involves using the data to perform a preliminary plant analysis to initiate preparation of other tasks of the PRA, followed by a plant visit (Task 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 Task 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 to assess likely fire scenarios before dominant accident sequences for internal events have been appropriately quantified and evaluated.

Task 1 – Obtain Analysis Information

Plant-Specific Information

Table 3-2 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 3-2, (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.

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. Three types of generic information that can be considered useful for supplementing the PRA are listed in Table 3-3.

Table 3-4 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.

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

Table 3-5 lists the plant information needed for an internal fire analysis.[1] Table 3-6 lists the information needed to perform an internal flood analysis. Basically, plant-specific flood incident

[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 3-2 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

Table 3-3 Generic information from plants of same/similar design

	Generic Information from Plants of Same/Similar Design	Examples
A	PRAs	Novovoronezh PRA
B	Analysis of Experienced Events	IAEA-TECDOC-749 on Generic Initiating Events for PRA for VVER Reactors
C	Component Failure Data Analysis	IAEA-TECDOC-478 on Component Reliability Data Sources in PRA

Table 3-4 Cross reference of PRA tasks and plant information needed

PRA Tasks	Plant Specific Information/Documentation Needed (Items from Table 3-1)	Generic Information for Plants of Similar Design (Items from Table 3-2)
Familiarization	All	All
Sources of Radioactive Releases	1,2,6,19	A,B,E,F
Select Plant Operating States	1,2,8	A
Definition of Core Damage	16	A,C
Selection of Initiating Events	1,2,7,9,12,14,17,19	A,B,E,F
Definition of Safety Function	1,2,7,9,14,16,19	A,B,C,E,F
Function/System Relationship	1,2,7,14,16,19	A,B,E
System Requirements	1,2,3,4,5,6,7,13,14,16,17,19	A,B,C,E,F
Grouping of Initiating Events	1,2,3,4,5,6,7,13,14,16,17,19	A,B,E
Event Sequence Modeling	1,2,6,7,9,12,14,16,19	A,B,C,E,F
System Modeling	1,2,3,4,5,6,7,13,14,16,17,19	A,B,D
Human Performance Analysis	1,2,6,7,9,12,14,16,18	A,B,E,F
Qualitative Dependence Analysis	123456719	A,B,E,F
Impact of Physical Process on Logic Model	1,2,7,9,12,14,16,17,19	A,B,C,E,F
Plant Damage State	Information needed for preceding tasks that provide input to the task	A,C
Analysis of Initiating Event Frequency	1,2,7,9,12,17,19	A,B,E,F
Component Reliability and Common Cause Failure	10,11,12,19	A,B,D,E,F
Assessment of Human Error Probabilities	1,2,6,7,9,12,14,16,18,19	A,B,E,F
Accident Sequence Boolean Equations	1,2,3,4,5,6,7,13,16,17,19	A,E
Initial Quantification of Accident Sequences	Information needed for preceding tasks that provide input to the task	A,D
Final Quantification of Accident Sequences	Information needed for preceding tasks that provide input to the task	A,D
Uncertainty Analysis	Information needed for preceding tasks that provide input to the task	A,D
Importance and Sensitivity Analyses	Information needed for preceding tasks that provide input to the task	A,E

Table 3-5 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 hydrant, 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 3-6 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)

data, potential sources of flood, and pathways from the flood sources to plant equipment are needed.

Table 3-7 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.

Table 3-7 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 ~ ½00,000), 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)

Task 2 – 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 3-3 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 Novovoronech 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.

Systems 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.

Task 3 – 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

[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.

model is developed that reliably reflects the plant design and operation. Frequent communications between the PRA team and the point of contact at 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.

3.1.4 Task Interfaces

This current task provides significant information to all of the analytical tasks of the PRA. The task provides basic information needed for the final documentation.

3.2 Level 1 Analysis

This section provides guidance for each of the analytical tasks associated with a Level 1 PRA for accidents initiated by internal events. Section 3.2.1 provides guidance for identifying initiating events internal to the plant and is closely related to Section 3.2.2, which describes accident sequence development. Section 3.2.2 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 Section 3.2.3. The systems analysis discussion includes guidance on system modeling, qualitative dependency analysis, and the assessment of spatial interactions. Section 3.2.4 describes the data analysis which includes assessments of initiating event frequencies, component reliability, and common-cause failure probabilities. The human reliability analysis is described in Section 3.2.5. Quantification, which includes initial and final quantification of the accident sequences, and sensitivity and importance analyses is discussed in Section 3.2.6.

3.2.1 Initiating Event Analysis

The objective of this activity 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 activity of a Level 1 probabilistic risk assessment (PRA). The initiating event analysis consists of identification and selection of events and grouping of these events.

3.2.1.1 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, or other environmental stresses. Floods (refer to Section 3.5) and fires (refer to Section 3.6) 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 re-flooding 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.

3.2.1.2 Products

The products for the identification and selection of initiating events task are:

- 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.
- 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).
- 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.

The products for the grouping of events task are:

- specific records of the grouping process including the success criteria for the final accident initiator groups.
- 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.

3.2.1.3 Analytical Tasks

The initiating event analysis consists of two task activities:

Task 1 – Identification and selection of events
Task 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 3.2.1.5.

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

Task 1 – 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.

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 3-8 and 3-9 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.

Reference to Previous Initiating Event List

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 3-9, taken from IAEA (1994), provides a list of generic initiators for VVER-1000 plants. Note that Table 3-10 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.

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 3.1 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.)

Table 3-8 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 3-9 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 3-10 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
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

[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 3-10 Generic list of initiating events for VVER-1000 reactors (IAEA, 1994) (cont'd)

General Categories	Initiating Events
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
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

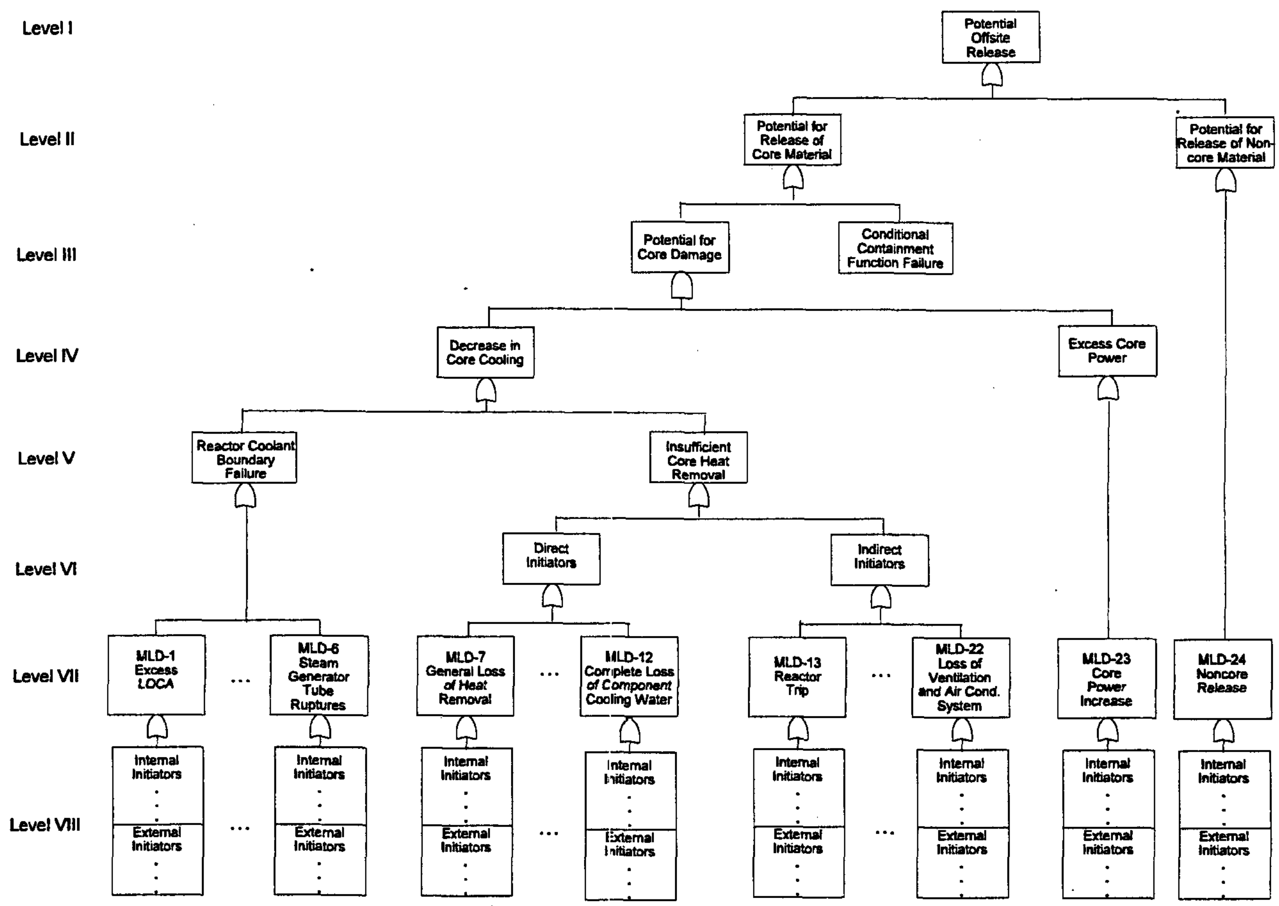

Figure 3.1 Master logic diagram

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 3.1. Level II represents the argument that such a release must be from either a damaged core or from another 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. 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.

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.

Task 2 -- 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: steam-line 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 front-line 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 operation 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 (Section 3.3).

- 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.

3.2.1.4 Task Interfaces

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.

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.

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.

3.2.1.5 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.

3.2.2 Accident Sequence Development

Accident sequence development consists of three interrelated tasks–namely, core damage definition, functional analysis and system success criteria, and event sequence modeling. 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 for plant 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.

3.2.2.1 Assumptions and Limitations

The delineation of the accident sequence ends with the determination of the status of the core as safe or damaged. The core is defined to be in a safe condition when the consequences of the radionuclide releases from the damaged fuel would be negligible. Realistically, core damage occurs when the allowable peak fuel cladding temperature is reached; however, using this definition involves detailed analyses beyond the scope of many studies, so a more conservative definition is often employed. For the Boiling Water Reactors (BWRs) in NUREG-1150, core damage is assumed to occur when the reactor water level is less than two feet above the bottom of the active fuel. Because Pressurized Water Reactors (PWRs) are not designed to allow steam cooling, core damage is assumed to occur at the time at which the top of the active fuel is uncovered. As knowledge of accident progression in the core evolves, less conservative assumptions concerning core damage may be used.

Plant system components modeled in a PRA are assumed to be fully operational or non-operational. Differentiation is not 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), only operation at nominal performance or inoperable.

The front-line systems used as event tree headings include only those systems present in the plant emergency operating procedures for responding to the initiating events defined for the analysis.

The Anticipated Transient Without Scram (ATWS) accident sequences for the BWRs are not always fully delineated. ATWS sequences in which the functions; reactor subcriticality, Reactor Coolant System (RCS) overpressure protection and inventory control, and core heating are successful, are assumed to be mitigated. Even if failure of the containment overpressure protection function occurs in an ATWS sequence following success of the other functions, the sequence frequency is often below the risk-significant cut-off value, and thus the sequence would be screened from the analysis.

ATWS sequences for PWRs are treated similar to those for BWRs. As with the BWRs, low sequence probabilities for ATWS scenarios prior to the need for containment overpressure protection would produce non-dominant sequences even if failure of containment overpressure protection was considered.

3.2.2.2 Products

The products for the core damage definition 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.

The products for the functional analysis and system success criteria task are:

- a definition of the safety functions to be modeled as top events in the event sequence analysis and the systems that provide those functions.

- a definition of the 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.

- a definition of new supporting analyses for initial success criteria selection.

- a definition success criteria resulting from the initial modeling effort.

The products of the event sequence modeling task are:

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

- 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.

3.2.2.3 Task Activities

Accident sequence development consists of three interrelated tasks:

Task 1 – Core damage definition,
Task 2 – Functional analysis and system success criteria, and
Task 3 – Event sequence modeling.

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 for plant 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.

Task 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.

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 (refer to Task 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 conservatism built into the definition, criteria, plant models, and analyses is 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.

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 Section 3.3.

Task 2 – Functional Analysis and System Success Criteria

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.

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).] Selection of success criteria is a continually evolving element in the PRA process (Bley, Buttemer, and Stetkar, 1988).

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 3-11, 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. 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 (Section 3.2.1), 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.

Activity 2 – Assessment of Function/System Relationship

The frontline systems 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 Section 3.1) 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 Section 3.1, 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 activity and provides the basis for many judgments that establish the success criteria.

Table 3-11 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

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, and a systematic assessment will ensure that the success criteria have adequate bases. The assessment should account for the definition of core damage, 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 4) 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:

1. Room heatup with no cooling;

2. Time until steam generator dryout following loss of feedwater;

3. 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.;

4. 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;

5. Possibility of pressurizer relief valves lifting following a variety of transients, accounting for realistic modeling of pressurizer steam space compression;

6. 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.;

7. 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;

8. Minimum success criteria for injection pumps following a variety of LOCAs; and

9. Pressurized thermal shock calculations under a variety of conditions.

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.

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:

1. Use conservative safety analyses on most scenarios;

2. Apply simplified analyses to develop preliminary, less conservative success criteria for scenarios that appear particularly sensitive;

3. Document the analyses and assumptions;

4. Evaluate the point estimate frequencies of the entire PRA model;

5. Review results to identify the dominant risk contributors; and

6. 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.

Task 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 (Section 3.2.1). 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.

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.

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.

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.

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.

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.

3.2.2.4 Task Interfaces

The core damage definition task (Task 1) has the following interfaces:

The functional analysis and system success criteria task (Task 2) has the following interfaces:

Plant Familiarization. Prior to the initial site visit, the plant safety functions should be defined. This information is essential background material for the site visit. During the site visit, a complete first draft of the dependency matrix must be completed.

Core Damage Definition. If the risk results (see Section 3.2.6.1, Initial Quantification of Accident Sequences) are found to be heavily dependent upon the precise definition of the state of core damage, then additional calculations 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 may suggest redefinition of the initiating event groups.

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

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

Human Reliability Analysis. Human reliability analysis is heavily dependent on Activity 3 (Task 2), 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 (Task 2) 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 (Task 2) 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 (Task 2) will be required to correct these problems.

The event sequence modeling task (Task 3) has the following interfaces:

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.

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. This task and the current task are highly coupled and performed in an iterative fashion. In Task 2 (Functional Analysis and Systems Success Criteria), Activity 1, Determination of Safety Functions, defines the safety functions to be modeled in the event trees. Task 2, Activity 2, Assessment of Function/System Relationships, provides the defining interrelationships among systems. Task 2, 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, Task 3 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. 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.

3.2.2.5 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.

3.2.3 Systems Analysis

The systems analysis consists of three interrelated tasks--namely, system modeling, subtle interactions, and spatial interactions. 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.

3.2.3.1 Assumptions and Limitations

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.

3.2.3.2 Products

The products of the system modeling task are:

- a portion of the "Systems Analysis" and the "Fault Tree" sections of the backup documentation.
- the system logic models in electronic form suitable for use in the sequence quantification activity.

The product of the subtle interactions task are:

- 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.

The product of the spatial interactions task are:

- 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.
- draft material for the final report. Specifically, a draft portion of the "Spatial Interactions" section 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

3.2.3.3 Analytical Tasks

Task 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.

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 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 3.2.

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:

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

	SUPPORT SYSTEMS										FRONTLINE SYSTEMS						
SUPPORT 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
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 3.2 Example of dependency matrix

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 Section 3.2.1), 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 Section 3.2.1. 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 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 3.3. 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 3.4) 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:

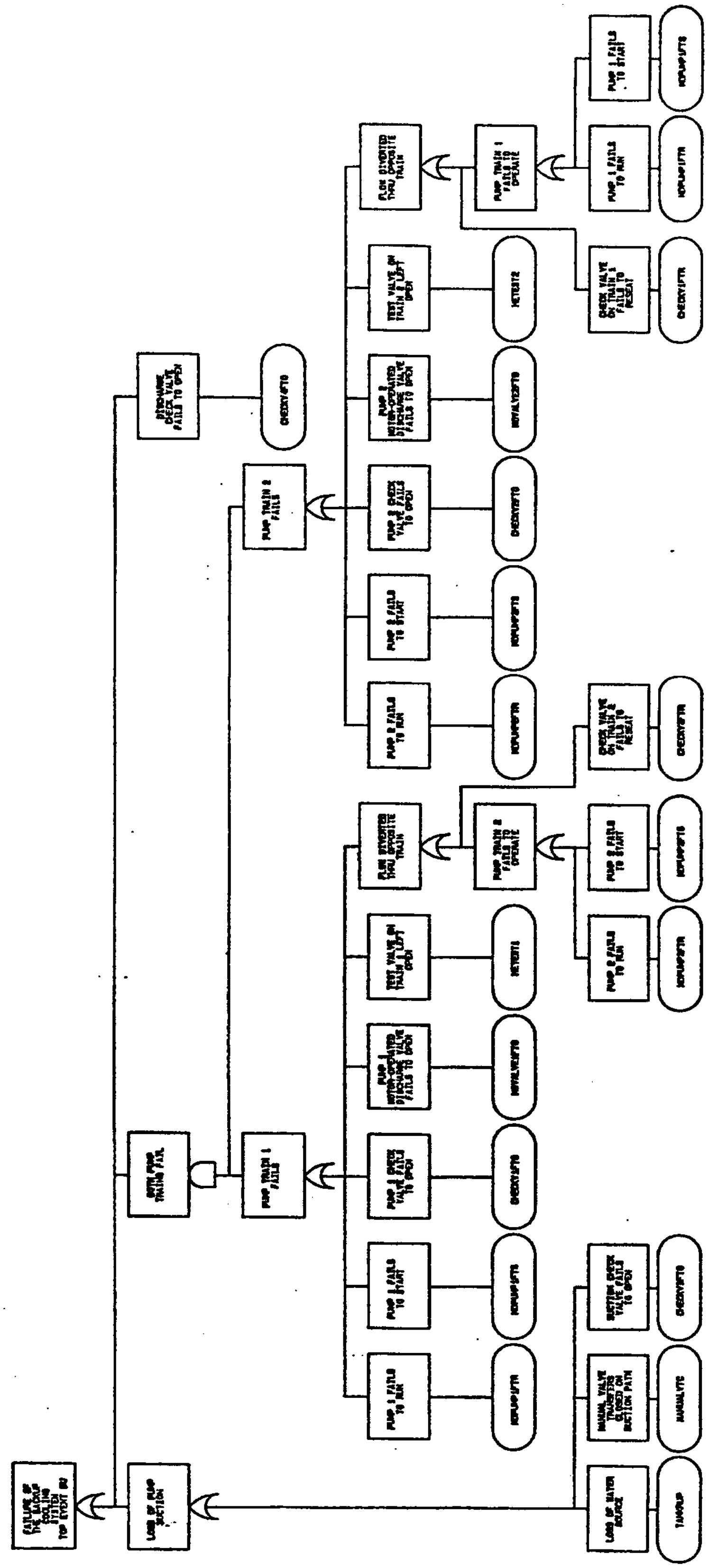

Figure 3.3 Example of fault tree for backup cooling system

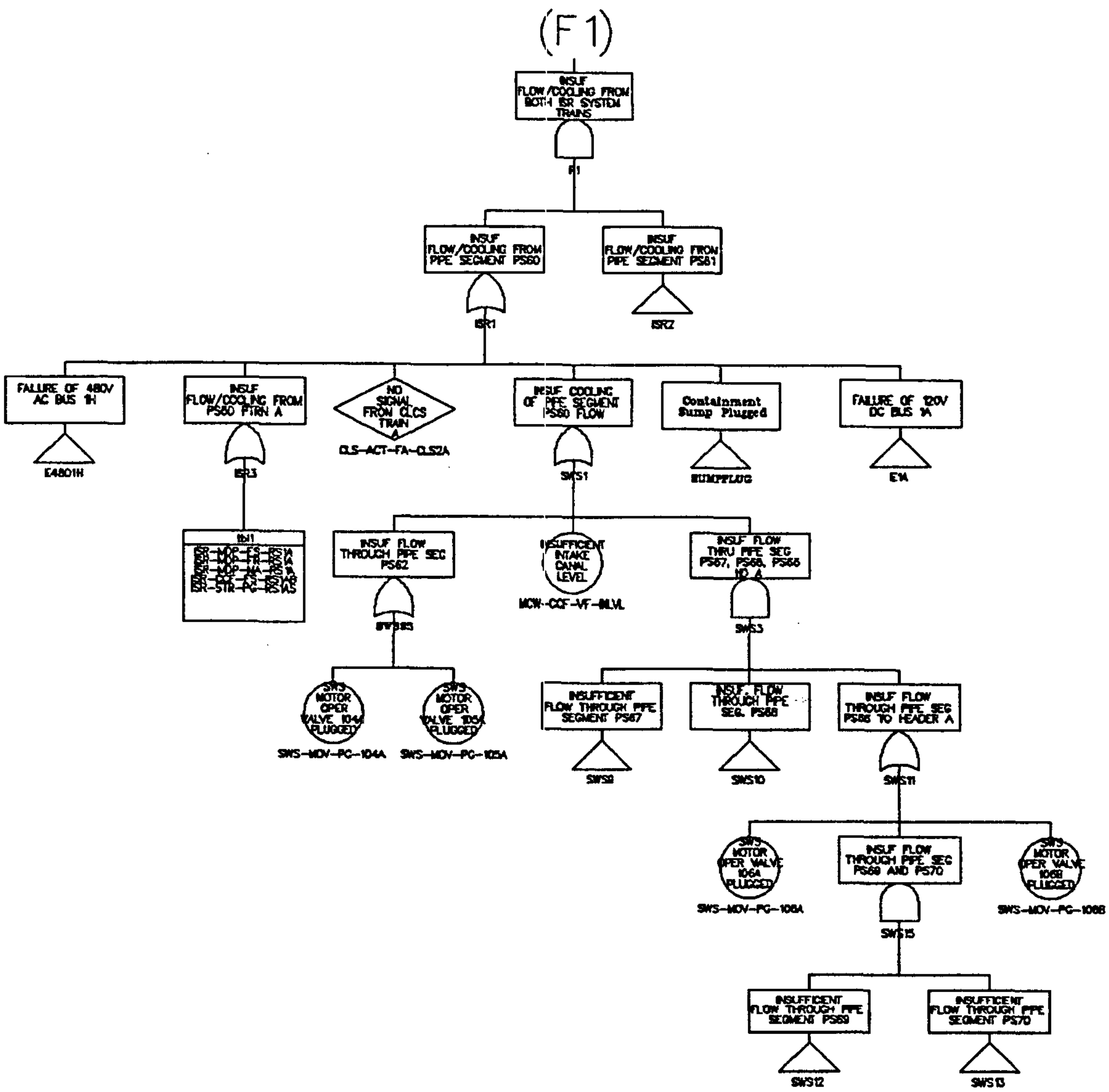

Figure 3.4 Example fault tree for inside spray recirculation

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:

   - 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 3.2.6.1 and 3.2.6.2).

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 3.2.3).

   - 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.

Task 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.

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 Section 3.2.5).

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.

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).

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.

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.

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.

Task 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 flood analysis (see Section 3.5) and fire analysis (see Section 3.6). The equipment location information is also used to support the assessment of seismic events (see Section 3.7).

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.

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.

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.

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 3-12 lists general types of equipment that are susceptible to damage if a particular hazard occurs in their location. Table 3-13 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
- 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.

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.

Table 3-12 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 3-13 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 3-12	

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.

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.

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 Sections 3.6 and 3.7) 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 3-14 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 3-14, the functional

Table 3-14 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.

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.

5. Hazard Mitigation Features. This entry briefly summarizes the hazard mitigation features that are present in the location. Table 3-15 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 3-14 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 3-14 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 3-14, the hazard occurrence frequency is actually assessed during the second phase of the internal plant hazard analysis. The frequency assessment process is described in Sections 3.6 and 3.7.

Table 3-15 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 3-12.	

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 Sections 3.6 and 3.7). 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.

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.

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.

3.2.3.4 Task Interfaces

Plant Familiarization. This task provides key source material for the system modeling, subtle and spatial interactions.

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.

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. 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. 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. 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.

3.2.3.5 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.

3.2.4 Data Analysis

Data analysis consists of three interrelated tasks—namely, determining (1) the frequency of initiating events, (2) component reliability, and (3) common-cause failure (CCF) probabilities. The first of these tasks quantifies the frequency of each group of initiating events identified in the task Initiating Event Analysis (refer to Section 3.2.1). 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.

3.2.4.1 Assumptions and Limitations

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.

3.2.4.2 Products

The products of the task on determining the frequency of initiating events are:

- material for the final report.
- the frequency information in electronic form suitable for use in the sequence quantification activity.

The component reliability task has two products:

- a generic component database based on generic WER 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.

- documentation including 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 task on estimating common-cause failure probabilities has the following products:

- 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.

- 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.

- 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.

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

3.2.4.3 Task Activities

Data analysis consists of the following three interrelated tasks–namely, determining (1) the frequency of initiating events, (2) component reliability, and (3) common-cause failure probabilities. Atwood (2003) provides additional guidance on the sources of information and methods available for estimating the parameters used in (1) and (2) above, including quantification of the uncertainties.

Task 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 (Section 3.2.1). 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.

The goal of this task is to develop a probabilistic description of the frequency of the initiating events of interest along with supporting documentation.

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.

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).

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.

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.

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 3.2.3).

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). 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.

Task 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).

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 3.2.3) and human reliability analysis (see Section 3.2.5). 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 maintenance. 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.

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.

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 3-16 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.

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 Task 1, Frequency of Initiating Events). 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

Table 3-16 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.

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 3-16. Note that all causes for performing corrective and preventive maintenance are included 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.

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.

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.

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 (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 .

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.

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.

Task 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.

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:

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

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).

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.

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.

Activity 4 – Initial Quantification

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

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.

Guidance is provided below for the following specific areas:

- 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.

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 A.

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.

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.

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.

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 3.5).

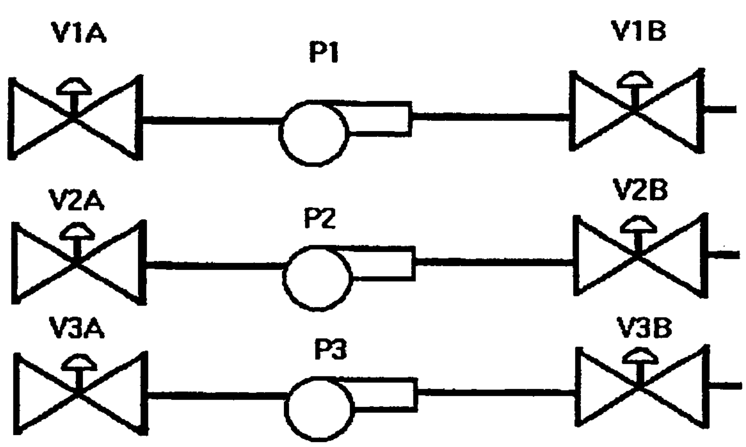

Figure 3.5 Simple example for CCF analysis

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 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 maintenance, 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.

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).

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.

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).

3.2.4.4 Task Interfaces

The task on determining the frequency of initiating events has the following interfaces:

- it requires input from the Initiating Event Analysis and provides output necessary for the Initial and Final Quantification of Accident Sequences.
- a more subtle interface is found with the task

- a more subtle interface is found with the task System Modeling. 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 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.

The component reliability task has the following interfaces:

Plant Familiarization. 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. 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. 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. 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. Component failure parameters, by providing input to system modeling, are indirect input needed for quantification of accident sequences.

The task related to determining common-cause failure (CCF) probabilities has the following interfaces:

- as discussed earlier, there is an explicit relationship between CCF modeling and the scope/level of detail in the PRA. There is also direct interaction between this task and the task System Modeling 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.
- the estimated CCF parameters are then used in the initial and final quantifications and sensitivity evaluations. 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 and for which this task would estimate CCF parameters.

3.2.4.5 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.

Atwood, C., et al., "Handbook of Parameter Estimation for Probabilistic Risk Assessment," NUREG/CR-6823, Sandia National Laboratories, September 2003.

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., "Defenses 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 Defenses 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.

3.2.5 Human Reliability Analysis

The objectives of the human reliability analysis (HRA) task are to identify, analyze, and quantify human failure events (HFEs), the PRA event tree/fault tree model basic events involving human actions. 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.

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 specific unsafe acts (UAs) and 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.

3.2.5.1 Assumptions and Limitations

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 pre-initiating event HFEs. Because 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 (Swain and Guttmann, 1983) and SLIM (Embry et al., 1984), focus on those actions 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 USNRC, NUREG-1624). 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 second-generation method, ATHEANA.

A limitation of all first-generation methods is that they are not structured to address the question of errors of commission or the search for challenging context. A second limitation is that the methods themselves do not provide guidance for the identification and prioritization of HFEs. Rather, HFEs drop out of the event tree analysis and quantification tasks, leading to a lack of consistency in the specific human actions addressed in similar PRAs.[3] Because of the importance of human UAs 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 UAs and EFCs in the ATHEANA methodology (USNRC, NUREG-1624) can be adapted to existing quantification approaches to enhance the value of the PRA.

ATHEANA was developed to increase the degree to which an HRA can realistically identify, represent, and quantify the kinds of human behaviors seen in accidents and near-miss events at nuclear power plants and at facilities in other industries that involve broadly similar kinds of human/system interactions. In particular, ATHEANA provides this improved capability by:

- more realistically searching for the kinds of human/system interactions that have played important roles in accident responses, including the identification and modeling of errors of commission (EOCs) and important dependencies, and by

- taking advantage of, and integrating, advances in psychology, engineering, plant operations, human factors, and probabilistic risk assessment (PRA) in its modeling and quantification.

As is common to all second generation methods, ATHEANA focuses on the context in which the operators must perform their function. Included in their focus on context is a systematic approach to identify important sources of dependency among human actions and between human actions and systems failures in the plant. Such interactions can couple human response to an entire sequence of seemingly independent cues, greatly increasing the likelihood of an HFE. All accident sequences which contain multiple HFEs should be examined for possible dependencies. If practical, HFEs which are completely dependent should be re-defined and modeled as a single event.

Finally, it is important to recognize that aspects of 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,

[3]The exception is SHARP1 (Wakefield, et al., 1992), a process for performing HRA (rather than a method for quantification) that provides guidance for the identification and prioritization of HFEs. Unfortunately, too few HRA analyses integrated their selected methods with the systematic SHARP1 process.

1983), will not apply to the HRA of Russian reactors. Therefore, while first-generation 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 (Forester, et al., 2002). For the post-initiating event HFEs, other alternatives should be considered. For example SLIM (Embrey et al., 1984) provides a structured approach for applying expert judgment based on the evaluation of PSFs for each HFE. The SLIM quantification could be enhanced by the thinking process of ATHEANA. This process entails evaluating the most-likely-to-be-significant UA-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 based on inapplicable experience.

The final methodology described below represents a compromise among competing factors including state-of-the-art methodologies, budget and schedule, practical limitations on the interaction between plant experts and analysts, and other practicalities of the project. Specific caveats are given for the approach used for quantification in Task 4. The basic steps of HRA performed in support of nuclear power plant PRA are similar for all approaches; in some methods they are explicitly included, others assume that the steps are performed as part of the PRA, before the HRA begins. In some methods they are rigorous, in others they are more intuitive. The guidance provided below for the KNPS HRA is consistent with the basic HRA process described in somewhat different terms in SHARP1, ATHEANA, and the IAEA HRA guidelines (IAEA Safety Series 50-P-10). Additional generic guidance on good practices to be employed in HRA is available (NRC, 2005) which promotes improved HRA quality.

3.2.5.2 Products

The results of each pre-initiating event HFE analysis will be documented in a report. This report will also detail the basis for quantification. If U.S. data, such as the tables for quantification in the Swain and Guttmann (1983) handbook, are used, it may be necessary to modify the probabilities to account for Russian and plant-specific characteristics.

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 and UAs for each HFE, and documenting the analysis 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 UA-EFC pairs identified for quantification and document the search process and associated analyst decisions.

The 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.

3.2.5.3 Task Activities

The primary discussion in this section 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.

This work is accomplished by completing the following five Tasks:

Task 1 Quantification of pre-initiating event HFEs,
Task 2 Development of a detailed list of post-initiating event HFEs,
Task 3 Development of a detailed list of significant context associated with each post-initiating event HFE,
Task 4 Quantification of post-initiating event HFEs,
Task 5 Recovery analysis.

Each of these tasks is discussed below. 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 3.2.6.1) and quantified in the final quantification (see Section 3.2.6.2). 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.

Task 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.

Swain (THERP) is the generally accepted method for determining pre-initiating event HFEs. The methods found in the handbook (Swain and Guttmann, 1983) shall therefore be followed.

Task 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 must be based on plant-specific design, capabilities, and priorities.

Task 3 – Development of a Detailed List of Significant Context Associated with Each Post-Initiating Event HFE

A number of PSFs could influence operator reliability, for example:

- Time of accident (day or night)
- Human interactions among personnel
- Scenario effect (the level of severity and difficulty the operator associates with the accident situation)

- Time available to make a decision and perform an action
- Level of operator knowledge
- Existence of training on a given scenario
- Quality of training
- Quality and availability of procedures
- Cognitive complexity
- Level of stress
- Human-machine interface.

Expert opinion, from plant operators, operations supervisors, and HRA analysts, can be used to develop an initial list of PSFs and to reduce the number of PSFs to those of most importance. Note that some factors vary by accident scenario and others are global as they are influenced by plant condition. Both types of factors should be considered for each post-initiating event HFE and structured into "decision tree" logic structures, with the PSFs used as top events. The decision tree is used in quantification and is shown as part of Task 4 below. Table 3-17 provides examples of PSFs used in the analysis and their definitions.

Task 4 – Quantification of Post-Initiating Event HFEs

As mentioned in the assumptions and limitations of Section 3.2.5.1, the approach for quantification represents a compromise among theoretical preferences and budget/schedule requirements as well as practicalities of the project including available expertise and limitations on the interaction between plant experts and analysts. The final approach used is a variation on the "decision tree" method (Spurgin, et al., 1980, and Bareith, et al., 1997). The approach is vulnerable to well-known theoretical objections, such as the PSF are not independent; their relationships to each other and to any probability anchors are dependent on plant conditions and specifics of each different scenario; lack of strong controls for bias and reliability; and no formal treatment of uncertainty is provided.

Pre-quantification qualitative analysis attempted to examine some of the issues of context described in second generation HRA methods and adaptations to the decision tree process attempted to account for dependencies. The benefits of the approach are that the issues important to HRA are well-examined qualitatively and can be used as the basis for improvements in the future.

The approach uses the following basic scheme and is more fully described in the references. Specifics of the final adaptations will be described in the KNPS final PRA report. Using the list of PSFs developed in the previous task, plant operations experts assign a weighting factor (referred to as a "K-factor") based on the perceived importance of each decision tree top event (selected PSF). A simplified example decision tree is given in Figure 3.6. Each branch under the top event is assigned a "K-value" between 1.0 (for the most beneficial branch) and that PSF's K-factor (for the most detrimental branch). Each path through the decision tree has an accumulated coefficients on an arbitrary scale, which are obtained by the multiplication of the applicable K-values for each branch path associated with that end-state. Note that the higher the coefficient, the more unlikely it is that the operators will successfully accomplish the required action.

The decision tree is used to evaluate specific HFE by having plant operations experts examine the required action against the logic of the tree. By answering the questions raised by the decision tree logic, such as "what is the effect of the scenario on the operator?", "How effective is the MMI in helping the operator?", and so on, a pathway for a particular HFE through the tree can be drawn, and a corresponding point on the decision tree scale (i.e., in the set of end-states) can be defined.

Calibration of the K-values to the probability of each HFE is accomplished by separately evaluating selected HFEs by other means and scaling the remaining events by the relationship between K-values and probabilities for the anchor events. Some adaptation of the K-values is possible to account for dependencies among the PSFs.

Task 5 – Recovery Analysis

The same process is used for the analysis of recovery actions as for the other post-initiating event HFEs as described in Tasks 3-5 above.

3.2.5.4 Task Interfaces

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.

3.2.5.5 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.

Bareith, A., et al., "Treatment of Human Factors for Improvements at the Paks Nuclear Power Plant," Proceedings of PSAM III, Crete, Greece (1997).

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.

Table 3-17 Example of performance shaping factors

Performance Shaping Factor	Potential Branches	Branch Definition
Available time (time interval from the first moment that the initiating event could begin until the moment when it would be no longer possible, accounting for the time to complete the initiating event)	Long	Time is sufficient to complete the action even if the decision on taking the action is not made when it first becomes possible to complete the initiating event.
	Middle	Time is more or less sufficient to complete the action even if the decision on taking the action is not made when it first becomes possible to complete the initiating event.
	Short	Time is insufficient or barely sufficient to complete the action if the decision on taking the action is not made quickly when it first becomes possible to complete the initiating event or time required to take action is comparable to the time available to complete the initiating event.
Scenario effect (influence of the emergency situation on the operator at the moment the initiating event is complete)	Easy	When the initiating event is completed, the parameters are not changing quickly, the process is stable, the stress level is not high, and the operator understands the situation and does not expect severe consequences.
	Medium	When the initiating event is completed, the parameters are changing more or less quickly, the stress level is medium, the process is not stable, and the operator understands the situation in general and may expect severe consequences.
	Severe	When the initiating event is completed, the parameters are changing quickly, there are extensive alarm and light signals occurring, the stress level is high, the process is not stable, and the operator may not understand the situation and expects severe consequences.
Cognitive complexity for decision making (cognitive complexity for making the decision on the need to complete an action, taking into account the impact of operator training on the initiating event)	Simple	The need to complete the action is obvious, and the operator has good training on the initiating event.
	Difficult	The need to complete the action is not clearly obvious, and the operator has some training on the initiating event.
	Very difficult	The need to complete the action is not obvious, and the operator has no training on the initiating event.

Table 3-17 Example of performance shaping factors (cont'd)

Performance Shaping Factor	Potential Branches	Branch Definition
Human-machine interface (quality and fitness of the human-machine interface associated with taking action on an initiating event, taking into account the quality of the information required to decide on the need to complete the initiating event)	Good	The human-machine interface for taking action in the face of the initiating event is well designed, the quality and fitness of the interface allows completion of the action without difficulties, one operator can complete the action, and the information required to make the decision to take the action is good.
	Adequate	The quality and fitness of the interface for taking action in the face of the initiating event is more or less adequate, and the information required to make the decision to take action is only adequate.
	Poor	The interface features are not well designed for taking action in the face of the initiating event, the operator expects considerable difficulties in taking action, more than one operator is needed to take action, and the information required to make the decision to take action is inadequate for understanding (or the information is absent entirely).
Quality of procedures (impact of the availability and quality of relevant procedures related to the initiating event)	Good	The initiating event is well described in the procedure, and the procedure is well known to the operator.
	Poor	The initiating event is poorly described or not described in the procedure, and the procedure is not well known to the operator.

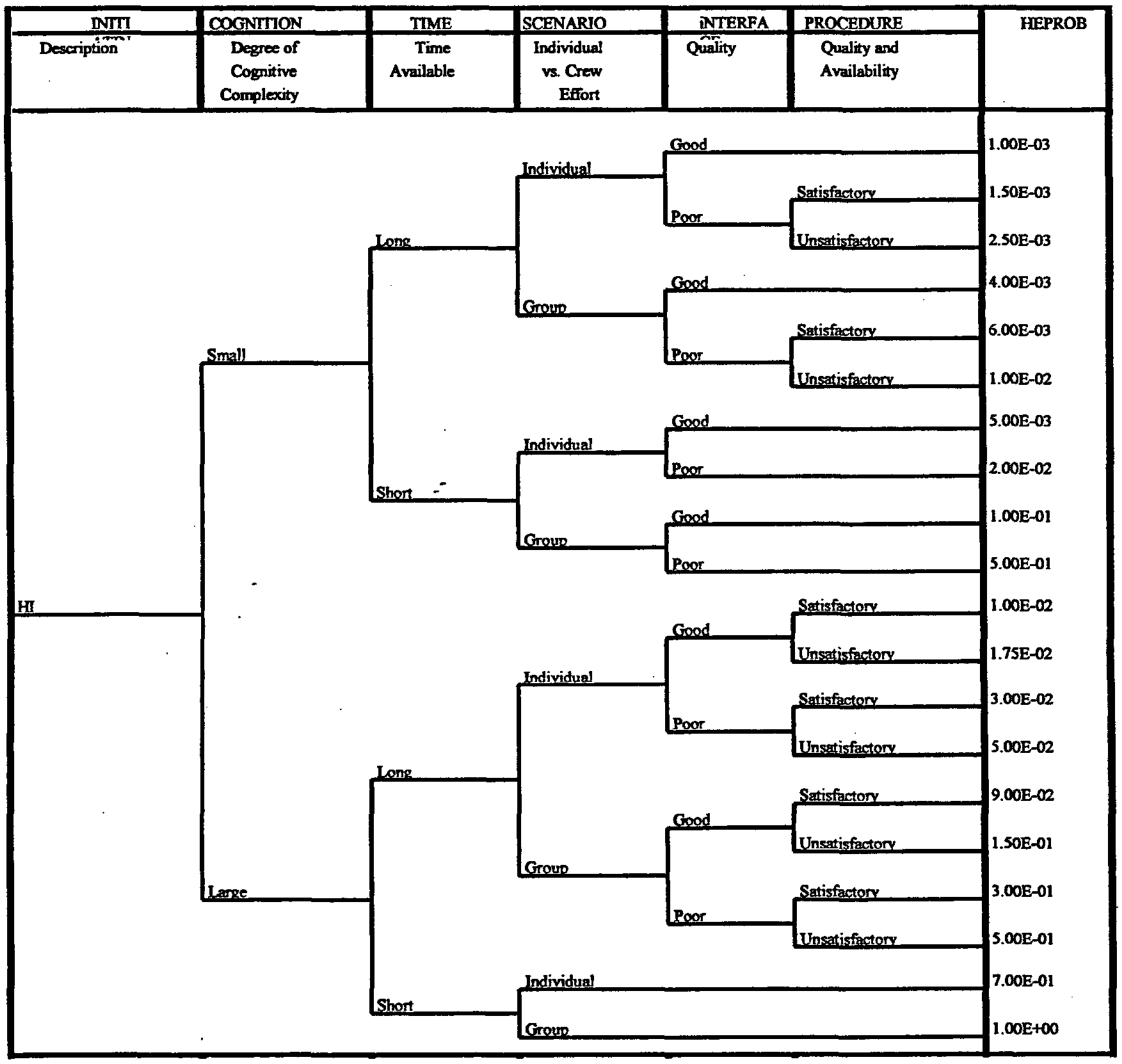

Figure 3.6 Example of a decision tree for performance shaping factors

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., 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.

Forester, J., Bley, D., Cooper, S., Kolazkowski, A., Lois, E., Siu, N., Thornsbury, E., and Wreathall, J., "Improved ATHEANA Quantification Process and Data Needs," to be published in proceedings of OECD/NEA Working Group WG-Risk Assessment: Building the New HRA: Strengthening the Link between Experience and HRA," Munich, Germany, January 2002.

IAEA, "Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants" Safety Series 50-P-10, 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.

Spurgin, A. J., et al., "Operator Reliability Experiments Using Power Plant Simulators," EPRI NP-6037, Electric Power Research Institute, Palo Alto, California (1990).

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.

USNRC, "Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)," NUREG-1624, Rev. 1, U.S. Nuclear Regulatory Commission, May 2000.

USNRC, "Good Practices for Implementing Human Reliability Analysis (HRA)," NUREG-1792, U.S. Nuclear Regulatory Commission, April 2005.

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.

Wakefield, D.J., G.W. Parry, A.J. Spurgin, and P. Moieni. "Systematic Human Action Reliability Procedure (Sharp) Enhancement Project, SHARP1 Methodology Report," EPRI TR-101711. Palo Alto, CA: Electric Power Research Institute, 1992.

3.2.6 Quantification and Results

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. 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.

3.2.6.1 Assumption and Limitations

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.

3.2.6.2 Products

The products of the task on initial quantification of accident sequences are:

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.

The products for the task on final quantification of accident sequences 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.

The products of the task on sensitivity and importance analyses are:

- 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.

3.2.6.3 Task Activities

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.

Task 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).

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.

2. System Success

Account for system success as necessary by using the approximation techniques mentioned below.

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.

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).

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.

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.

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.

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.

Task 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.

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.

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.

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.

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.

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.

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.

Common-Cause Modeling

Based on the preliminary accident sequence quantification and on sensitivity and importance results, the common-cause quantification is reviewed (see Section 3.2.4), 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.

Task 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).

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.

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.

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 Section 3.2.5), 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 3.2.4), 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.

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.

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.

3.2.6.4 Tasks Interfaces

The task related to initial quantification has the following interfaces:

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.

The task related to final quantification has the following interfaces:

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. 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 Section 3.3) which in turn provides source term information to the consequence and risk integration task (refer to Section 3.4). Whether or not Level 2/3 analyses are performed depends on the scope of the PRA (refer to Chapter 2).

The task related to sensitivity and importance analyses has the following interfaces:

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.

3.2.6.5 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.

3.3 Level 2 Analysis (Probabilistic Accident Progression and Source Term Analysis)

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 that damages the reactor core. To satisfy this objective, a Level 2 PRA couples two major elements of analysis to a completed Level 1 PRA:

1. A structured and comprehensive evaluation of 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 leakage from the containment pressure boundary.

Figure 3.7 illustrates each of these elements and indicates how they relate to each other conceptually.

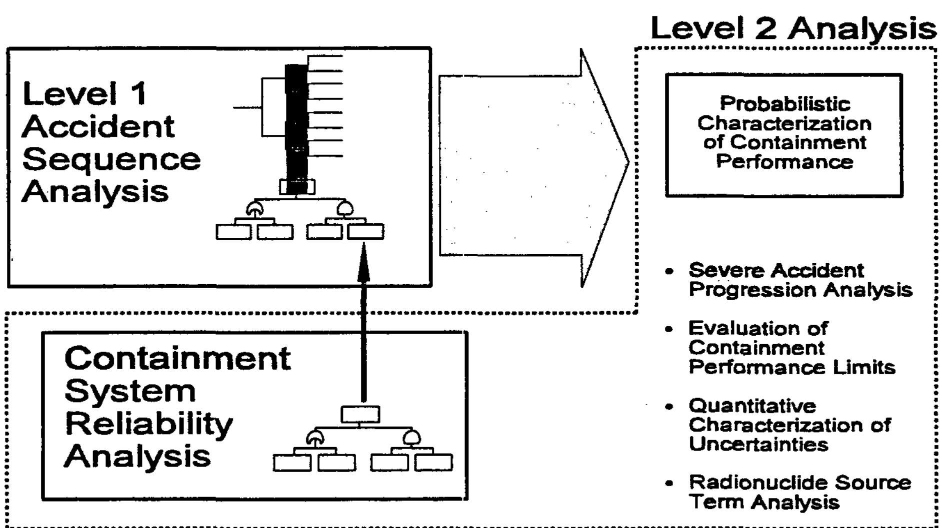

Figure 3.7 Relationship among the major parts of a Level 2 PRA

In an earlier version of this procedure guide (NUREG/CR-6572, Vol. 3 Part 1) the attributes of a simplified approach to conducting the analyses associated with each of the technical elements was presented. This simplified approach is reproduced in Appendix B.

In the current version of the procedures guide the attributes of comprehensive Level 2 PRA are presented. A detailed description of the attributes of conducting the technical analyses associated with a comprehensive Level 2 PRA is provided below.

One type of containment performance assessment in response to such accidents would be to perform a deterministic calculation with a validated, first-principles model of accident progression. Such a calculation would generate a time-history of loads imposed on the containment pressure boundary. These loads would then be compared against structural performance limits of the containment. If the loads exceed the performance limits, the containment would be expected to fail; conversely, if the performance limits surpass the calculated loads, the containment would be expected to survive. In such an assessment, the overall frequency of accidents resulting in a release to the environment would simply be the frequency of accident sequences in which the calculated containment loads exceed the performance limits.

Unfortunately, neither the current knowledge regarding many aspects of severe accident progression nor (albeit to a lesser extent) the knowledge regarding containment performance limits is sufficiently precise to conduct such an analysis. Rather, in a PRA, an assessment of containment performance is performed in a manner that explicitly considers imprecise knowledge of severe accident behavior, the resulting challenges to containment integrity, and the capacity of the containment to withstand various challenges. Therefore, the potential for a release to the environment is typically expressed in terms of the conditional probability of containment failure (or bypass) for the spectrum of accident sequences (determined from Level 1 PRA analysis) that proceed to core damage.

Figure 3.8 indicates how the conditional probability of containment failure is calculated. For each Level 1 core damage accident sequence (frequency, F_i), the probability of the various containment failure modes are calculated. For example, the probability of early containment failure (ef_i), containment bypass (bp_i), late containment failure (lf_i) and no containment failure (nf_i) are determined. For the example shown in Figure 3.8, Accident Sequence 1 completely bypasses the containment and thus the conditional probability of bypass given the occurrence of this accident is unity. These characteristics could result from an accident such as an interfacing system LOCA. Alternatively, Accident Sequence 2 could result in several different containment failure modes or no containment failure. For this accident, the probability of early failure (0.5) could be caused by several mechanisms such as overpressure, shell melt-through and others. Containment bypass (0.1) could be the result of induced steam generator tube rupture (for PWRs only). Whether the containment fails late (0.2) or not at all (0.2) depends on several factors including the operability of containment heat removal systems. Once the probabilities of these containment failure modes has been determined for each accident sequence, the probabilities conditional on total core damage are calculated.

The probability of early containment failure conditional on core damage ($CCFP_{ef}$) is determined by summing (i=1→n) the early failure probabilities for all accident sequence weighted by their respective frequencies (F_i). The summation is then divided by the total core damage frequency (CDF).

$$CCFP_{ef} = \frac{\sum_{i=1}^{n} [ef_i][F_i]}{CDF}$$

A similar approach is used to determine the conditional probabilities of bypass accidents, late containment failure and no containment failure.

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 off-site 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 off-site consequences (i.e., health effects, property damage, etc.), which are estimated in the Level 3 portion of a PRA (refer to Section 3.4).

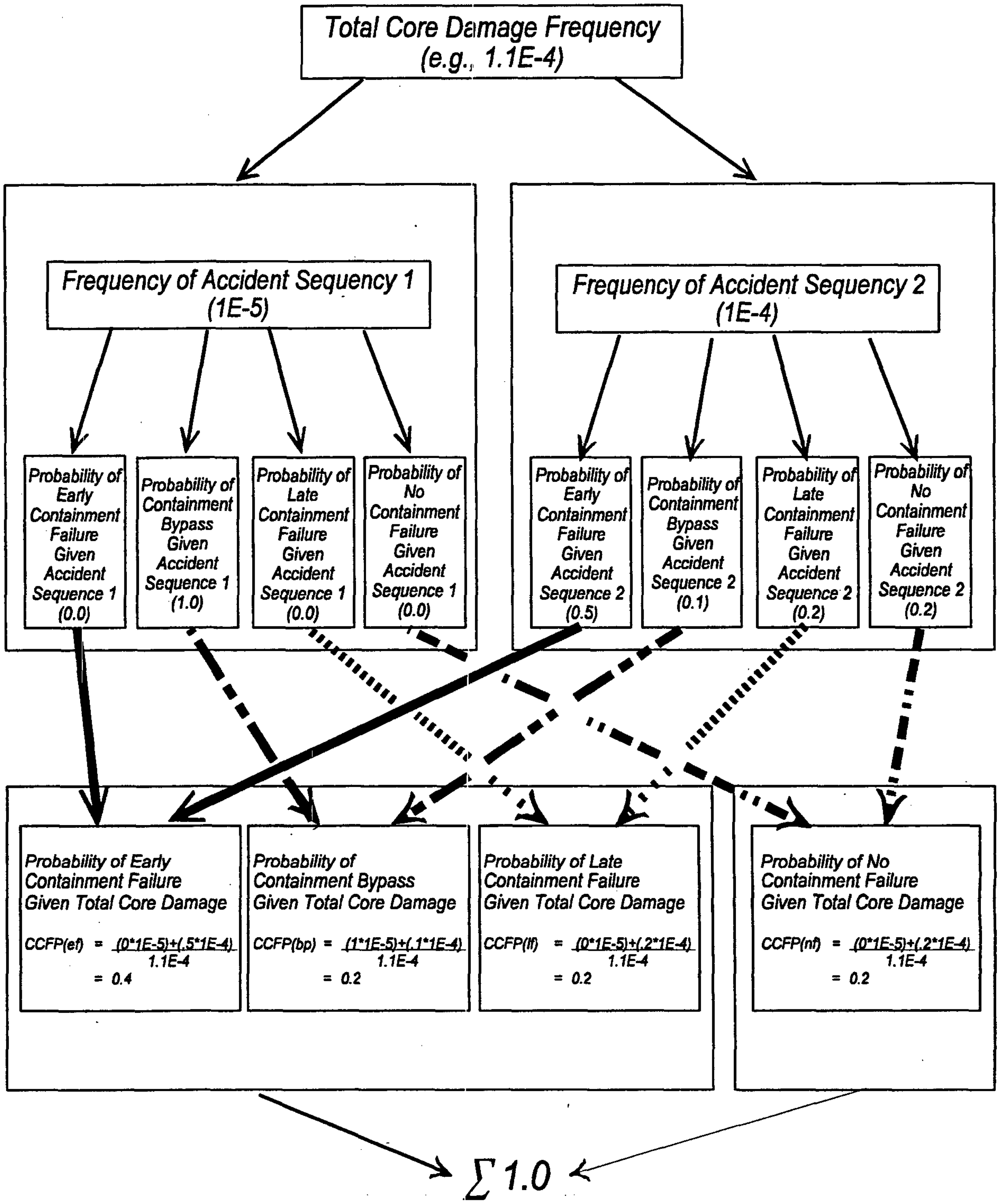

Figure 3.8 Conditional probability of containment failure

This section describes the attributes of a Level 2 PRA analysis, emphasizing the scope and level of detail associated with major elements of a Level 2 analysis, rather than the specific methods used to assemble a probabilistic model. This approach is deliberately used because several different methods have been used to generate and display the probabilistic aspects of severe accident behavior and containment performance. By far, the most common methods are those that use standard event and/or fault tree logic structures; however, some practitioners use other techniques. Further, the specific way in which ostensibly similar logic structures are organized and solved (numerically) can differ substantially from one study to another, primarily as a result of differences in quantification techniques and associated computer software offered by vendors of PRA services. In principle, any of these methods can be used to produce a Level 2 PRA provided that they encompass the scope and level of detail described below.

As indicated above, the two major technical activities of a Level 2 PRA are (1) determination of the conditional probability of containment failure or bypass for accident sequences that proceed to core damage and (2) a characterization of the radiological source term to the environment for each sequence resulting in containment failure or bypass. These major technical activities are however composed of several component parts:

- Plant Damage State Determination
- Assessing Containment Challenges
- Containment Performance Characterization
- Containment Probabilistic Characterization
- Radionuclide Release Characterization
- Quantification of Results

Each of these technical activities are discussed in the following section.

3.3.1 Plant Damage State Determination

The primary objective of this task of a Level 2 PRA is to characterize the type and severity of challenges to containment integrity that may arise during postulated severe accidents. An analysis to determine these characteristics acknowledges the dependence of containment response on details of the accident sequence. Therefore, a critical first step is developing a structured process for defining the specific accident conditions to be examined. Attributes have to be determined of reducing the large number of accident sequence developed for Level 1 PRA analysis to a practical number for detailed Level 2 analysis.

3.3.1.1 Assumption and Limitations

Because of the diversity and redundancy of safety systems designed to prevent and/or mitigate potential accident conditions in a nuclear plant, multiple failures must occur for an accident to proceed far enough to damage the reactor fuel. The primary purpose of a Level 1 PRA analysis is to identify the specific combinations of system or component failures (i.e., accident sequence cut sets) that would allow core damage to occur.

Unfortunately, the number of cut sets generated by a Level 1 analysis is very large (typically greater than 10,000). It is impractical to evaluate severe accident progression and resulting containment loads for each of these cut sets. As a result, the common practice is to group the Level 1 cut sets into a sufficiently small number of "plant damage states" to allow a practical assessment of the challenges to containment integrity resulting from the full spectrum of accident sequences.

3.3.1.2 Products

In general, sufficient information should be provided to allow an independent analyst to reproduce the results. At a minimum, the following products are expected

- a thorough description of the procedure used to group (bin) individual accident sequence cut sets into plant damage states, or other reduced set of accident scenarios for detailed Level 2 analysis

- a listing of the specific attributes or rules used to group cut sets

- a listing and/or computerized data base providing cross reference for all cut sets to plant damage states and vice versa

3.3.1.3 Analytical Tasks

This technical activity involves two tasks:

1. Defining PDS Characteristics
2. PDS Binning

Each of these tasks are described in detail in the following sections.

Task 1 – Defining PDS Characteristics

The number of plant damage states produced by this grouping (or "binning") process cannot be established a priori. Rather, a Level 2 PRA first defines the attributes of an accident sequence that represent important initial or boundary conditions to the assessment of severe accident progression or containment response or characteristics of system operation that can have an important effect on the resulting environmental source term. Example attributes are shown in Table 3-18.

Table 3-18 Example attributes for grouping accident sequence cut sets

Attribute	Possible states
Accident Initiator	• Large, Intermediate, or Small LOCAs • Transients • LOCA outside the containment pressure boundary • Steam Generator Tube Rupture
Reactor Coolant System (RCS) Pressure at the Onset of Core Damage	• High • Low
Status of Emergency Coolant Injection Systems	• Operate in injection mode, but fail upon switchover to recirculation cooling • Fail to operate in injection mode
Status of Steam Generators (PWRs)	• Auxiliary feedwater operates/fails • Secondary isolated/depressurized
Status of Residual Heat Removal Systems	• Operate • Failed
Status of Containment at Onset of Core Damage	• Isolated • Not isolated
Status of Containment Safeguard Systems	• Sprays always operate/fail or are available if demanded • Sprays operate in injection mode, but fail upon switchover to recirculation cooling • Fan coolers always operate/fail or are available if demanded • Containment venting system(s) operate/fail • Hydrogen control system(s) operate/fail

The functional effect of the specific failures represented by the terms in each accident sequence cut set are then mapped into possible plant damage states according to the binning attributes. There is no "unique" list of attributes against which this exercise should be conducted for a Level 2 analysis; Table 3-18 simply provides examples, not an exhaustive list. A comprehensive list of attributes for representative PWR and BWR Level 2 analyses can be found in NUREG/CR-4551, Volume 3 (Breeding, 1990) and Volume 4 (Payne, 1990), respectively. Although many of these attributes can be applied generically across many different reactor/containment designs, special attributes are often necessary to address plant-specific design features (e.g., isolation condenser operation in certain BWRs.) In a Level 2 PRA, any characteristic of the plant response to a given initiating event that would influence either subsequent containment response or the resulting radionuclide source term to the environment is represented as an attribute in the plant damage state binning scheme. These characteristics include the following:

- ***The status of systems that have the capacity to inject water to either the reactor vessel or the containment cavity.*** Defining system status simply as "failed" or "operating" is not sufficient in a Level 2 analysis. Low-pressure injection systems may be available but not operating at the onset of core damage because they are "dead-headed" (i.e., reactor vessel pressure is above their shutoff head). Such states are distinguished from "failed" low-pressure injection to account for the capability of dead-headed systems to discharge after reactor vessel failure (i.e., providing a mechanism for flooding the reactor cavity).

- ***The status of systems that provide heat removal from the reactor vessel or containment.*** Careful attention is paid to the interactions between such systems and the coolant injection systems. For example, the status properly accounts for limitations in the capability of dual-function systems such as the RHR system in most BWRs (which provides pumping capacity for LPCI and heat removal for suppression pool cooling).

- ***Recoverability of "failed" systems after the onset of core damage.*** Typical recovery actions include restoration of AC power to active components and alignment of nonsafety-grade systems to provide (low-pressure) coolant injection to the reactor vessel or to operate containment sprays. Constraints on recoverability (such as no credit for repair of failed hardware) are defined in a manner that is consistent with recovery analysis in the Level 1 PRA.

- ***The interdependence of various systems for successful operation.*** For example, if successful operation of a low-pressure coolant injection system is necessary to provide adequate suction pressure for successful operation of a high-pressure coolant injection system, failure of the low-pressure system (by any mechanism) automatically renders the high-pressure system unavailable. This information may only be indirectly available in the results of the Level 1 analysis, but is explicitly represented in the plant damage state attributes if recovery of the low-pressure system (after the onset of core damage) is modeled.

Task 2 – PDS Binning

Several subtle aspects of the mapping of accident sequence cut sets from the Level 1 analysis to plant damage states used as input to a Level 2 analysis are worth noting at this point:

- The entire core damage frequency generated by the Level 1 accident sequence analysis is carried forward into the Level 2 analysis. The reason for conserving the CDF is to allow capture of the risk contribution from low-frequency, high-consequence accident sequences.

- The mapping is performed at the cut set level, not the accident sequence level. There are several reasons for this level of detail:

  – Depending on the level of detail represented in the Level 1 accident sequence event trees, it may be impossible to properly capture the effects of support system failures and other dependencies among the various binning attributes without reviewing the basic events that caused a system failure.

- Recovery of failed systems after the onset of core damage is considered in the containment performance assessment of a Level 2 PRA. For this activity to be modeled correctly, system failures that are "recoverable" are distinguished from failures that are "not recoverable." This information typically lies only within the sequence cut sets. Note that the definition of recoverable is consistent with the recovery analysis performed in the Level 1 PRA.

- To appropriately model human reliability related to operator actions that occur after the onset of core damage, information regarding prior operator performance (i.e., prior to the onset of core damage) is carried forward from the Level 1 analysis. Again, this information typically lies only within sequence cut sets.

• For some accident sequences, the status of all systems may not be determined from the sequence cut sets. For example, if the success criteria for a large break LOCA in a PWR require successful accumulator operation, the large LOCA sequence cut sets involving failure of all accumulators will contain no information about the status of other coolant injection systems. However, realistic resolution of the status of such systems often provides a mechanism for representing accident sequences that are arrested before substantial core damage and radionuclide release occur. In a Level 2 analysis, these systems are not simply assumed to operate as designed. Rather, their failure frequencies are estimated in a manner that preserves relevant support system dependencies. These are then numerically combined with the sequence cut set frequency from the Level 1 analysis.

3.3.1.4 Task Interfaces

This task is the critical interface between the Level 1 and Level 2 portions of the PRA. The entire core damage frequency generated by the Level 1 PRA is carried forward into the Level 2 analysis. The various core damage accident sequences are grouped into a smaller number of plant damage states for processing through the Level 2 analysis. These plant damage states are defined so that all of the accident sequences grouped into a particular plant damage state can be treated the same in terms of accident progression analysis. The output of this task is a set of plant damage states with the corresponding frequencies.

3.3.1.5 References

Breeding, R. J., et al., "Evaluation of Severe Accident Risks: Surry Unit 1," NUREG/CR-4551, Volume 3, SAND86-1309, Sandia National Laboratories, October 1990.

Payne, A. C., et al., "Evaluation of Severe Accident Risks: Peach Bottom Unit 2," NUREG/CR-4551, Volume 4, SAND86-1309, Sandia National Laboratories, December 1990.

3.3.2 Assessing Containment Challenges

This Level 2 PRA task has two objectives:

1. Assess the reliability of containment systems during severe accidents, and

2. Characterize severe accident progression and the attendant challenges to containment integrity.

3.3.2.1 Assumptions and Limitations

The reliability of systems whose primary function is to maintain containment integrity during accident conditions is incorporated into the accident sequence analysis performed during a Level 1 PRA. Such systems may include containment isolation, fan coolers, distributed sprays, and hydrogen igniters. An assessment of the reliability of these systems is incorporated into a Level 2 analysis to ascertain whether they would operate as designed to mitigate containment response during core damage accidents. The methods, scope, and technical rigor used to evaluate the reliability of these systems are comparable to those used in the Level 1 analysis of other "front-line" systems (refer to Section 3.2.3).

The element of a Level 2 PRA that often receives the most attention is the evaluation of severe accident progression and the attendant challenges to containment integrity. This is because considerable time and effort can be spent performing computer code calculations of dominant accident sequences. Further, exercising broad-scope accident analysis codes [such as the Modular Accident Analysis Program (MAAP) (EPRI, 1994) or MELCOR (Summers, 1994) provides the only framework within which the important interactions among severe accident phenomena can be accounted for in an integrated fashion. Consequently, the results of these calculations typically form the principal basis for estimating the timing of major accident events and for characterizing a range of potential containment loads.

Although code calculations are an essential part of an evaluation of severe accident progression, their results do not form the sole basis for characterizing challenges to containment integrity in a Level 2 PRA. There are several reasons for this:

1. Many of the models embodied in severe accident analysis codes address highly uncertain phenomena. In each case, certain assumptions are made (either by the model developers or the code user) regarding controlling physical processes and the appropriate formulation of models that represent them. In some instances, the importance of these assumptions can be tested via parametric analysis. However, the extent to which the results of any code calculation can be demonstrated to be robust in light of the numerous uncertainties involved is severely limited by practical constraints of time and resources. Therefore, the assumptions inherent in many code models remain untested.

2. None of the integral severe accident codes contain models to represent all accident phenomena of interest. For example, models for certain hydrodynamic phenomena such as buoyant plumes, intra-volume natural circulation, and gas-phase stratification, are not represented in most integral computer codes. Similarly, certain severe accident phenomena, such as dynamic fuel-coolant interactions (i.e., steam explosions) and hydrogen detonations, are not represented.

3. It is simply impractical to perform an integral calculation for all severe accident sequences of interest.

As a result, the process of evaluating severe accident progression involves a strategic blend of plant-specific code calculations, applications of analyses performed in other prior PRAs or severe accident studies, focused engineering analyses of particular issues, and experimental data. The manner in which each of these sources of information are used in a Level 2 PRA is described below.

3.3.2.2 Products

In general, sufficient information in the documentation of assessing containment system challenges is provided to allow an independent analyst to reproduce the results. At a minimum, the following information is documented:

For the activities related to assessing the reliability of containment systems:

- a description of information used to develop containment systems' analysis models and link them with other system reliability models (This documentation is prepared in the same manner as that generated in Level 1 analysis of other systems as discussed Section 3.2.3).

For the activities related to characterizing severe accident progression:

- a description of plant-specific accident simulation models (e.g., for MAAP [EPRI, 1994] or MELCOR [Summers, 1994]) 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 a 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 assuming applicability of results

- 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

3.3.2.3 Analytical Tasks

This technical activity involves two tasks:

1. Containment System Analysis
2. Evaluation of Severe Accident Progression

Each of these tasks are described in detail in the following sections.

Task 1 – Containment System Analysis

Fault tree models (or other techniques) for estimating failure probabilities are developed and linked directly to the accident sequence models from the Level 1 PRA. This linkage is necessary to properly capture the important influence of mutual dependencies between failure mechanisms for containment systems and other systems. Obvious examples include support system dependencies, such as electrical power, component cooling water, and instrument/control air. Other dependencies that need to be represented in a manner consistent with the Level 1 system models are more subtle, however, as illustrated by the following examples:

- Indirect failure of containment systems caused by harsh environmental conditions (resulting from failure of a support system) are represented in the assessment of containment system reliability. An example is failure of reactor or auxiliary building room cooling causing the failure of containment systems because of high ambient temperatures.

- The influence of containment system operation prior to the onset of core damage is accounted for in the evaluation of system operability after the onset of core damage. For example, consider an accident sequence in which containment sprays successfully initiate on an automatic signal early in an accident sequence. If later in the sequence (but prior to the onset of core damage) emergency operating procedures direct reactor operators to terminate containment spray operation to allow realignment of emergency coolant injection systems, the configuration of the containment spray system (and thus its reliability) differ from a sequence in which containment sprays would not have been demanded prior to the onset of core damage.

- The human reliability analysis associated with manual actuation of containment systems (e.g., hydrogen igniters) accounts for operator performance during earlier stages of an accident sequence. This analysis follows the same practices used in the Level 1 analysis as described in Section 3.2.5.

The long-term performance of containment systems is also evaluated although the issues to be considered may differ substantially from those listed above. This evaluation accounts for degradation of the environment within which systems are required to operate as an accident sequence proceeds in time. Examples of factors that may arise after the onset of core damage include:

- loss of net positive suction head (NPSH) for coolant pumps due to suppression pool heat up in BWRs
- plugging of fan cooler inlet plena as a result of the accumulation of aerosols (generated perhaps as a consequence of core-concrete interactions) in PWRs
- failure of systems with components internal to the containment pressure boundary as a result of high temperatures or pressure associated with hydrogen combustion

In all cases, the assessment of failure probability for containment systems are based on realistic equipment performance limits rather than bounding (design-basis or equipment qualification) criteria.

Task 2 – Evaluation of Severe Accident Progression

The following are used to determine the number of plant specific calculations that would be performed using an integral code to support a Level 2 PRA:

- At least one integral calculation (addressing the complete time domain of severe accident progression) is performed for each plant damage state. However, this may not be practical depending on the number of plant damage states developed according to the above discussion. At a minimum, calculations are performed to address the dominant accident sequences (i.e., those with the highest contribution to the total core damage frequency). Calculations are also performed to address sequences that are anticipated to result in relatively high radiological releases (e.g., containment bypass scenarios).
- In addition to the calculations of a spectrum of accident sequences described above, several sensitivity calculations are performed to examine the effects of major uncertainties on calculated accident behavior. For example, multiple calculations of a single sequence are performed in which code input parameters are changed to investigate the effects of alternative assumptions regarding the timing of stochastic events (such as operator actions to restore water injection), or the models used to represent uncertain phenomena (such as the size of the opening in containment following over-pressure failure). These calculations provide information that is essential to the quantitative characterization of uncertainty in the Level 2 probabilistic logic models (refer to the discussion of logic model development and assignment of probabilities below).

Table 3-19 lists phenomena that can occur during a core meltdown accident and which involve considerable uncertainty. This list was based on information in NUREG-1265 (NRC, 1991), NUREG/CR-4551 (Gorham-Bergeron, 1993) and other studies. It is recognized that considerable disagreement persists within the technical community regarding the magnitude (and in some cases, the specific source) of uncertainty in several of the phenomena listed in Table 3-19. A major objective of the expert panels assembled as part of the research program that culminated in NUREG-1150 (NRC, 1990) was to translate the range of technical opinions within the severe accident research community into a quantitative measure of uncertainty in specific technical issues. In a Level 2 PRA, the results of this effort are used as guidance for defining the range of values of uncertain modeling parameters to be used in the sensitivity calculations described above.

Table 3-19 Severe accident phenomena

Phenomena	Characteristics of accident phenomena
Hydrogen generation and combustion	• Enhanced steam generation from melt/debris relocation • Steam starvation caused by degraded fuel assembly flow blockage • Clad ballooning • Recovery of coolant injection systems • Steam/hydrogen distribution within containment • De-inerting due to steam condensation or spray operation
Induced failure of the reactor coolant system pressure boundary	• Natural circulation flow patterns within the reactor vessel upper plenum, hot legs, and steam generators • Creep rupture of hot leg nozzles, pressurizer surge line, and steam generator U-tubes
Debris bed coolability and core-concrete interactions	• Debris spreading/depth on the containment floor • Crust formation at debris bed surface and effects on heat transfer • Debris fragmentation and cooling upon contact with water pools • Steam generation and debris oxidation
Fuel coolant interactions	• Potential for dynamic loads to bounding structures • Hydrogen generation during melt-coolant interaction
Melt/debris ejection following reactor vessel failure	• Melt/debris state and composition in the lower head • Mode of lower head failure • Debris dispersal and heat transfer following high-pressure melt ejection

A fundamental design objective of the integral severe accident analysis codes used to support Level 2 PRA (e.g., MAAP, MELCOR) is that they be fast running. Efficient code operation is necessary to allow sensitivity calculations to be performed within a reasonably short time and with minimal resources. One consequence of this objective, however, is that many complex phenomena are modeled in a relatively simple manner or, in some cases, are not represented at all. Therefore, a state-of-the-art Level 2 PRA addresses the inherent limitations of integral code calculations in two respects. First, the importance of phenomena not represented by the integral codes are evaluated by some other means (i.e., either application of specialized computational models or experimental investigation). Secondly, the effects of modeling simplification are examined by comparisons with mechanistic code calculations.

There are obvious practical benefits to applying or adapting results of completed studies of severe accident progression in other plants to the PRA of interest. If the applicability of such studies can be demonstrated, substantial savings can be achieved by eliminating unnecessary (repetitive) analysis. Application of analyses from studies of similar plants is common in Level 2 PRAs. However, such analyses can not completely supplant the plant-specific evaluations described above.

The prerequisite for applying results of studies for another plant is a demonstration of similarity in plant design and operational characteristics such that the same results would be generated if plant-specific analyses were performed. Demonstration of similarity involves a direct comparison of key plant design features and, if necessary, scaling analysis. Examples of features to be included in such a comparison are listed in Table 3-20. The effects of differences in these design features is examined, and techniques for adapting or scaling the results of the surrogate analyses developed.

Table 3-20 Example plant design/operational parameters to be compared to demonstrate similarity for use as surrogate analysis

Component	Design characteristics of component
Reactor Core	• Nominal Power • Number of Fuel Assemblies • Number of Fuel Rods per Assembly • Core Mass (UO_2, Cladding, Misc. support structures)
Reactor Vessel	• Inside Diameter • Height • Nominal Operating Pressure • Number of Safety/Pressure Relief Valves • Safety / Relief Valve relief valve design flow rate • Reactor Coolant System Liquid Volume
Containment	• Total Free Volume • Design Pressure • Nominal Internal Operating Pressure • Atmosphere composition • Reactor Cavity Floor Area • Penetration arrangement and construction • Water Capacity before Spill-over into Reactor Cavity • Concrete (floor) composition

In summary, evaluating severe accident progression involves a complex process of plant-specific sensitivity studies using integral codes, mechanistic code calculations, use of prior calculations, experimental data and expert judgement. Examples of this process are given in Appendix B for each of the phenomena listed in Table 3-19 above.

3.3.2.4 Task Interfaces

Task 1 assesses the reliability of containment systems for those severe accidents identified in the Level 1 PRA. Fault tree models (or other techniques) for estimating failure probabilities are developed and linked directly to the accident sequence models from the Level 1 PRA.

Task 2 has a critical interface with the plant damage state determination (refer to Section 3.3.1). For each of the plant damage states defined in Section 3.3.1, an evaluation of the severe accident progression would be performed in Task 2.

The output of these tasks is used together with the analyses performed in Section 3.3.3 to develop a range of potential containment failure modes and their corresponding frequencies.

3.3.2.5 References

EPRI, "MAAP4 - Modular Accident Analysis Program for LWR Power Plants, "RP3131-02, Volumes 1-4, Electric Power Research Institute, 1994.

Summers, R. M., et al., "MELCOR Computer Code Manuals - Version 1.8.3," NUREG/CR-6119, SAND93-2185, Volumes 1-2, Sandia National Laboratories, 1994.

NRC, "Uncertainty Papers on Severe Accident Source Terms," NUREG-1265, U.S. Nuclear Regulatory Commission, 1991.

Gorham-Gergeron, E. D., et al., "Evaluation of Severe Accident Risks: Methodology for the Accident Progression, Source Term, Consequence, Risk Integration, and Uncertainty Analyses," NUREG/CR-4551, SAND86-1309, Sandia National Laboratories, December 1993.

NRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, Volume 1, Main Report, U.S. Nuclear Regulation Commission, 1990.

3.3.3 Containment Performance Characteristics

The objective of this element of a Level 2 PRA is to determine the limits (or capacity) that the containment can withstand given the range and magnitude of the potential challenges. These challenges take many forms, including internal pressure rises (that occur over a sufficiently long time frame that they can be considered "static" in terms of the structural response of the containment), high temperatures, thermo-mechanical erosion of concrete structures, and under some circumstances, localized dynamic loads such as shock waves and internally generated missiles. Realistic estimates for the capacity of the containment structure to withstand these challenges are generated to provide a metric against which the likelihood of containment failure can be estimated.

3.3.3.1 Assumptions and Limitations

A thorough assessment of containment performance generally begins with a structured process of identifying potential containment failure modes (i.e., mechanisms by which integrity might be violated). This assessment commonly begins by reviewing a list of failure modes identified in PRAs for other plants to determine their applicability to the current design. Such a list was incorporated into NUREG-1335 (NRC, 1989), the NRC's guidance for performing an IPE. This review is then supplemented by a systematic examination of plant-specific design features and emergency operating procedures to ascertain whether additional, unique failure modes are conceivable. For each plausible failure mode, containment performance analyses are performed using validated structural response models, as well as plant-specific data for structural materials and their properties.

Unfortunately, current models for the response of complex structures to even "simple" loads (such as internal pressure) are not sufficiently robust to allow simultaneous prediction of a failure threshold and resulting failure size. This is particularly true for structures composed of non-homogeneous materials with highly non-linear mechanical properties such as reinforced concrete. As a result, calculations to establish performance limits are supplemented with information from experimental observations of containment failure characteristics and expert judgment. Examples of this process can be found in Task 2 below.

3.3.3.2 Products

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 over-pressure 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
- 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

3.3.3.3 Analytical Tasks

This technical activity involves two tasks:

1. Containment Structural Analysis
2. Containment Failure Mode Analysis

Each of these tasks are described in detail in the following sections.

Task 1 – Containment Structural Analysis

In a Level 2 PRA, the attributes of the analyses necessary to characterize containment performance limits are consistent with those of the containment load analyses against which they will be compared:

- They focus on plant-specific containment performance (i.e., application of reference plant analyses is generally inadequate).

- They consider design details of the containment structure such as:

  - containment type (free-standing steel shell; concrete-backed steel shell; pre-stressed, post-tensioned, or reinforced concrete)
  - the full range of penetration sizes, types, and their distribution (equipment and personnel hatches, piping penetrations, electrical penetration assemblies, ventilation penetrations)
  - penetration seal configuration and materials
  - discontinuities in the containment structure (shape transitions, wall anchorage to floors, changes in steel shell or concrete reinforcement)

- They consider interactions between the containment structure and neighboring structures (the reactor vessel and pedestal, auxiliary building(s), and internal walls).

For many containment designs, over-pressure has been found to be a dominant failure mechanism. In a state-of-the-art Level 2 PRA, the evaluation of ultimate pressure capacity is performed using a plant-specific, finite-element model of the containment pressure boundary including sufficient detail to represent major discontinuities such as those listed above. The influence of time-varying containment atmosphere temperatures is taken into account by performing the calculation for a reasonable range of internal temperatures. To the extent that internal temperatures are anticipated to be elevated for long periods of time (e.g., during the period of aggressive core-concrete interactions), thermal growth and creep rupture of steel containment structures is taken into account.

Task 2 – Containment Failure Mode Analysis

The characterization of containment performance limits is not simply a matter of defining a threshold load at which the structure "fails." A Level 2 PRA attempts to distinguish between structural damage that results in "catastrophic failure" of the containment from damage that results in significant leakage[4] to the environment. Leakage is often characterized by a smaller opening (i.e., one that may not preclude subsequent increases in containment pressure). Failure to isolate the containment is also considered. It is very important to assess both the location and size of the containment failure because of the implications for the source term calculation, e.g., given the same in-vessel and ex-vessel releases inside containment, a rupture in the drywell of a Mark II containment would typically result in higher releases to the environment than a leak in the wetwell.

The NUREG-1150 Expert Panel for Structural Response Issues assessed the containment overpressure failure issue for the Peach Bottom (Payne, 1990), Sequoyah (Gregory, 1990), Surry (Breeding, 1990) and Zion plants (Park, 1993). The assessments of the expert panel are documented in NUREG/CR-4551, Volume 2, Part 3 (Breeding, 1990). Two of these plants have free-standing steel containments and two have reinforced concrete containments. In addition to the distributions the expert panel provided for overpressure failure loads for these containment

[4]Significant leakage is defined relative to the design basis leakage for the plant. Leakage rates greater than 100 times the design basis have been found risk significant in past studies.

probabilities for failure location and failure mode (leak, rupture or catastrophic rupture). Both containment types were considered to be vulnerable to the propagation of cracks into ruptures. For a single containment, the panel assessed the conditional probability of multiple failure locations and sizes. For example, six different location/size failures (failure modes) were obtained for overpressure failure for the Peach Bottom containment: (1) wetwell leak, (2) rupture, no suppression pool bypass (discontinuity strains at T-stiffeners), (3) wetwell rupture, suppression pool bypass (membrane failure), (4) drywell leak (bending strain at the downcomers), (5) drywell head leak (gasket failure), and (6) drywell rupture (in main body near penetration due to loss of concrete wall back support).

Failure location and size by dynamic pressure loads and internally generated missiles are also probabilistically examined. The structural response expert panel for NUREG-1150 assessed the size and location of the containment breach by dynamic pressure loads for Grand Gulf (Brown, 1990) (reinforced concrete) and Sequoyah (free-standing steel). Both leaks and ruptures were predicted to occur in the containment response to detonations at Grand Gulf, and ruptures were predicted to occur at Sequoyah. Alpha mode failure (for all NUREG-1150 plants) and steel shell melt-through of a containment wall by direct contact of core debris (for Peach Bottom and Sequoyah) were treated as rupture failures of containment in NUREG-1150.

Basemat melt-through is generally treated as a leak in most Level 2 PRAs because of the protracted times involved as well as the predicted radionuclide retention in the soil. If a bypass of containment, such as an interfacing systems LOCA, is predicted to occur, then its effective size and location (e.g., probability that the break is submerged in water) are also estimated in order to perform the source term calculations.

3.3.3.4 Task Interfaces

These tasks have a critical interface with assessing containment challenges (refer to Section 3.3.2). For each of the plant damage states defined in Section 3.3.1, an evaluation of the severe accident progression would be performed in Task 2 of Section 3.3.2. This information is needed to characterize containment performance.

The output of these tasks is used together with the analyses performed in Section 3.3.2 to develop a range of potential containment failure modes and their corresponding frequencies.

3.3.3.5 References

NRC, "Individual Plant Examination: Submittal Guidance," NUREG-1335, U.S. Nuclear Regulatory Commission, August 1989.

NRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, U.S. Nuclear Regulatory Commission, December 1990.

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.

Brown, T. D., et al., "Evaluation of Severe Accident Risks: Grand Gulf Unit 1," NUREG/CR-4551, Volume 6, SAND86-1309, Sandia National Laboratories, December 1990.

Payne, A. C., "Evaluation of Severe Accident Risks: Peach Bottom Unit 2," NUREG/CR-4551, Volume 4, SAND86-1309, Sandia National Laboratories, December 1990.

Gregory, J. J., et al., "Evaluation of Severe Accident Risks: Sequoyah Unit 1," NUREG/CR-4551, Volume 5, SAND86-1309, Sandia National Laboratories, December 1990.

Park, C. K., "Evaluation of Severe Accident Risks: Zion Unit 1," NUREG/CR-4551, Volume 7, BNL-NUREG-52029, Brookhaven National Laboratory, March 1993.

3.3.4 Containment Probabilistic Characterization

3.3.4.1 Assumptions and Limitations

One feature that distinguishes a state-of-the-art Level 2 PRA from other, less comprehensive assessments is the way in which uncertainties are represented in the characterization of containment performance[5]. In particular, explicit and quantitative recognition is given to uncertainties in the individual processes and parameters that influence severe accident behavior and attendant containment performance. These uncertainties are then quantitatively integrated by means of a probabilistic logic structure that allows the conditional probability of containment failure to be quantitatively estimated, as well as the uncertainty in the containment failure probability.

Two elements of such an assessment are described below. First, the characteristics of the logic structure (i.e., containment event tree) used to organize the various contributors to uncertainty are described. However, the major distinguishing element of a full-scope approach to characterizing containment performance is the manner in which the CET is quantified. That is whether or not uncertainty distributions for major events are assigned and propagated through the logic model. The key phrase here is uncertainty distributions (i.e., point estimates of probability are not universally applied to the logic model). Characteristics of these distributions and the manner in which they are used in a typical logic model are described later in this section.

3.3.4.2 Products

The following documentation is generated to describe the process by which the conditional probability of containment failure is calculated:

- a listing and description of the structure of the overall logic model used to assemble the probabilistic representation of containment performance (Graphical displays of events 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
- a description of the computer program used to exercise the logic model and calculate final results

[5]Uncertainties in the estimation of fission product source terms are also represented in a full-scope Level 2 PRA; however, this topic is discussed in Section 3.3.5.

3.3.4.3 Analytical Tasks

This technical activity involves two tasks:

1. Containment Event Tree Construction
2. Containment Event Tree Quantification

Each of these tasks is described in detail in the following sections.

Task 1 – Containment Event Tree Construction

The primary function of a "containment event tree," or any other probabilistic model evaluating containment performance, is to provide a structured framework for organizing and ranking the alternative accident progressions that may evolve from a given core damage sequence. In developing this framework, whether it be in the form of an event tree, fault tree or other logic structure, several elements are necessary to allow a rigorous assessment of containment performance:

- Explicit recognition of the important time phases of severe accident progression. Different phenomena may control the nature and intensity of challenges to containment integrity and the release and transport of radionuclides as an accident proceeds in time. The following time frames are of particular interest to a Level 2 analysis:
    - After the initiating event, but before the onset of core damage. This time period establishes important initial conditions for containment response after core damage begins.
    - After the core damage begins, but prior to failure of the reactor vessel lower head. This period is characterized by core damage and radionuclide release (from

fuel) while core material is confined within the reactor vessel.

- Immediately following reactor vessel failure. Prior analyses of containment performance suggest that many of the important challenges to containment integrity occur immediately following reactor vessel failure. These challenges may be short-lived, but often occur only as a direct consequence of the release of molten core materials from the reactor vessel immediately following lower head failure.

- Long-term accident behavior. Some accident sequences evolve rather slowly and generate relatively benign loads to containment structures early in the accident progression. However, in the absence of some mechanism by which energy generated within the containment can be safely rejected to the environment, these loads may steadily increase to the point of failure in the long-term.

When linked end-to-end, these time frames constitute the outline for most probabilistic containment performance models. Within each time frame, uncertainties in the occurrence or intensity of governing phenomena are systematically evaluated.

- Consistency in the treatment of severe accident events from one time frame to another. Many phenomena may occur during several different time frames of a severe accident. However, certain limitations apply to the composite (integral) contribution of some phenomena over the entire accident sequence and these are represented in the formulation of a probabilistic model.

A good example is hydrogen combustion in a PWR containment. Hydrogen generated during core degradation can be released to the containment over several time periods. However, an important contribution to the uncertainty in containment loads generated by a combustion event is the total mass of hydrogen involved in a particular combustion event. One possibility is that hydrogen released to the containment over the entire in-vessel core damage period is allowed to accumulate without being burned (perhaps) as a result of the absence of a sufficiently strong ignition source. Molten core debris released to the reactor cavity at vessel breach could represent a strong ignition source, which would initiate a large burn (assuming the cavity atmosphere is not steam inert). Because of the mass of hydrogen involved, this combustion event might challenge containment integrity. Another possibility is that while the same total amount of hydrogen is being released to the containment during in-vessel core degradation, a sufficiently strong ignition source exists to cause several small burns to occur prior to vessel breach. In this case, the mass of hydrogen remaining in the containment atmosphere at vessel breach would be very small in comparison to the first case, and the likelihood of a significant challenge to containment integrity at that time should be correspondingly lower. Therefore, the logic for evaluating the probability of containment failure associated with a large combustion event occurring at the time of vessel breach is able to distinguish these two cases and preclude the possibility of a large combustion event if hydrogen was consumed during an earlier time frame.

- Recognition of the interdependencies of phenomena. Most severe accident phenomena and associated events require certain initial or boundary conditions to be relevant. For example, a steam explosion can only occur if molten core debris comes in contact with a pool of water. Therefore, it may not be meaningful to consider ex-vessel steam explosions during accident scenarios in which the drywell floor (BWR) or reactor cavity (PWR) is dry at the time of vessel breach. Logic models for evaluating containment performance capture these and many other such interdependencies among severe accident events and phenomena. Explicit representation of these interdependencies provides the mechanism for allowing complete traceability between a particular accident sequence (or plant damage state) and a specific containment failure mode.

Task 2 – Containment Event Tree Quantification

There are many approaches to transforming the technical information concerning containment loads and performance limits to an estimate of failure probability, but three approaches appear to dominate the literature. In the first (least rigorous) approach, qualitative terms expressing various degrees of uncertainty are translated into quantitative (point estimate) probabilities. For example, terms such as "likely" or "unlikely" are assigned numerical values (such as 0.9 and 0.1). Superlatives, such as "very" likely or "highly" unlikely, are then used to suggest degrees of confidence that a particular event outcome is appropriate. The subjectivity associated with this method is controlled to some extent by developing rigorous guidelines for the amount and quality of information necessary to justify progressively higher confidence levels (i.e., probabilities approaching 1.0 or 0.0). Nonetheless, this method is not considered an appropriate technique for assigning probabilities to represent the state of knowledge uncertainties (such uncertainties tend to dominate a Level 2 PRA, rather than uncertainty associated with random behavior.) in a PRA. Among its weaknesses, this approach simply produces a point estimate of probability and is not a rigorous technique for developing probability distributions.

The second technique involves a convolution of paired probability density functions. In this technique, probability density functions are developed to represent the distribution of credible values for a parameter of interest (e.g., containment pressure load) and for its corresponding failure criterion (e.g., ultimate pressure capacity). This method is more rigorous than the one described above in the sense that it explicitly represents the uncertainty in each quantity in the probabilistic model. The basis for developing these distributions is the collective set of information generated from plant-specific integral code calculations, corresponding sensitivity calculations, other relevant mechanistic calculations, experimental observations, and expert judgment. The conditional probability of containment failure (for a given accident sequence) is then calculated as the intersection of the two density functions (see Figure 3.9).

While this technique provides an explicit treatment of uncertainty at intermediate stages of the analysis, it still ultimately generates a point estimate for the probability of containment failure caused by a particular mechanism.

The contributions to (and magnitude of) uncertainty in the final (total) containment failure probability is discarded in the process.

The third technique involves adding an additional feature to the technique described above. That is, the probability density functions representing uncertainty in each term of the containment performance logic model are propagated throughout the entire model to allow calculation of statistical quantities such as importance measures. One means for accomplishing this objective is the application of Monte Carlo sampling techniques (such as Latin Hypercube). The application of this technique to Level 2 PRA logic models, pioneered in NUREG-1150 (NRC, 1990), accommodates a large number of uncertain variables.

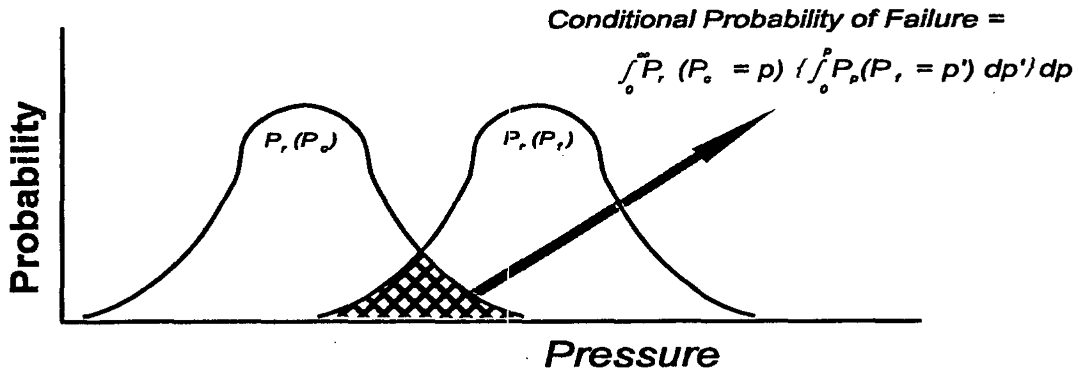

Figure 3.9 Probability density functions for containment peak pressure (P_c) and failure pressure (P_f)

Other techniques have been developed for specialized applications, such as the direct propagation of uncertainty technique developed to assess the probability of containment failure as a result of direct containment heating in a large dry PWR. However, these other techniques are constrained to a small number of variables and are not currently capable of applications involving the potentially large number of uncertain variables addressed in a Level 2 PRA.

3.3.4.4 Task Interfaces

These tasks have a critical interface with the evaluation of the severe accident progression (refer to Task 2 of Section 3.3.2).

The output of these tasks is a range of potential containment failure modes and their corresponding frequencies which provide input to radionuclide release characterization (Section 3.3.5).

3.3.4.5 References

NRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, U.S. Nuclear Regulatory Commission, December 1990.

3.3.5 Radionuclide Release Characterization

The second, albeit equally important, product of a Level 2 PRA is a quantitative characterization of radiological release to the environment resulting from each accident sequence that contributes to the total core damage frequency.

The specific manner in which radionuclide source terms are characterized in a Level 2 analysis is described first. Attributes of coupling the evaluation of radionuclide release to analyses of severe accident progression for particular sequences are also described. Finally, attributes of addressing uncertainties in radionuclide source terms are described.

3.3.5.1 Assumptions and Limitations

In many Level 2 analyses, the characterization of radiological release is used solely as a semi-quantitative scale to rank the relative severity of accident sequences. In such circumstances, a rigorous quantitative evaluation of radionuclide release, transport, and deposition may not be necessary. Rather, order-of-magnitude estimates of the size of release for a few representative radionuclide species provide a satisfactory scale for ranking accident severity. In a state-of-the-art Level 2 PRA, however, the characterization of radionuclide release to the environment provides sufficient information to completely define the "source term" for calculating off-site health and economic consequences for use in a Level 3 PRA.

Further, the rigor required of the evaluation of radionuclide release, transport, and deposition directly parallels that used to evaluate containment performance:

- Source term analyses (deterministic computer code calculations) reflect plant-specific features of system design and operation. In particular, the models used to calculate radionuclide source terms faithfully represent plant-specific characteristics such as fuel, control material, and in-core support structure composition and spatial distribution; configuration and deposition areas of primary coolant system and containment structures; reactor cavity (or drywell floor) configuration and concrete composition; and topology of transport pathways from the fuel and/or core debris to the environment.

- Calculations of radionuclide release, transport, and deposition represent sequence-specific variations in primary coolant system and containment characteristics. For example, reactor vessel pressure during in-vessel core melt progression and operation (or failure) of containment safeguard systems such as distributed sprays are represented in a manner that directly accounts for their effects on radionuclide release and/or transport. The procedure for organizing the numerous accident sequences generated in a Level 1 PRA into a reasonably small number of groups that exhibit similar radionuclide release characteristics is described below.

- Uncertainties in the processes governing radionuclide release, transport, and deposition are quantified. Uncertainties related to radionuclide behavior under severe accident conditions are quantified to characterize uncertainties in the radionuclide source term associated with individual accident sequences. This is achieved in the same way uncertainties for the phenomena governing severe accident progression are used to characterize uncertainty in the probability of containment failure (described below).

3.3.5.2 Products

In general, sufficient information of the documentation of analyses performed to characterize radiological source terms is provided that allows an independent analyst to reproduce the results. At a minimum, the following information is documented for a PRA:

- a summary of all computer code calculations used as the basis for estimating plant-specific source terms for selected accident sequences

- a description of modeling methods used to perform plant-specific source term calculations including a description of the method by which source terms are assigned to accident sequences for which computer code (i.e., MAAP [EPRI, 1994] or MELCOR [Summers, 1994]) 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

- a description of the method by which uncertainties in source terms are addressed

- 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

3.3.5.3 Analytical Tasks

This technical activity involves three tasks:

1. Definition of Radionuclide Source Terms
2. Coupling Source Term and Severe Accident Progression Analyses
3. Treatment of Source Term Uncertainties

Each of these tasks is described in details in the following sections.

Task 1 – Definition of Radionuclide Source Terms

The analysis of health and economic consequences resulting from an accidental release of radionuclides from a nuclear plant (in a Level 3 PRA) requires specification of several parameters (from a Level 2 PRA) that define the environmental source term. Ideally, the following information is developed:

- the time at which a release begins
- the time history of the release of all radioisotopes that contribute to early (deterministic) and late (stochastic) health consequences
- the elevation (above local ground level) at which the release occurs
- the energy with which the release is discharged to the environment
- the size distribution of radioactive material released in the form of an aerosol (i.e., particulate)

As in many other aspects of a comprehensive PRA, it is impractical to generate this information for the full spectrum of accident conditions produced by Level 1 and 2 analyses. To address this constraint, several simplifications are made in a Level 2 analysis. In particular, the following assumptions are typically made regarding the radioactive material of interest:

- All isotopes of a single chemical element are released from fuel at the same rate.
- Chemical elements exhibiting similar properties in terms of their measured rate of release from fuel, physical transport by means of fluid advection, and chemical behavior in terms of interactions with other elemental species and bounding structural surfaces can be effectively modeled as one composite radionuclide species. Typically, the specific properties of a single (mass dominant) element are used to represent the properties of all species within a group.

The combination of these two assumptions leads to a radionuclide grouping scheme that reduces the total number of modeled radionuclide species to nine groups, as shown in Table 3-21.

Although the species listed above are released from fuel in their elemental form, it is firmly established that many species quickly combine with other elements to form compounds as they migrate away from the point of release. The formation of these compounds and the associated change in the physio-chemical properties of individual radionuclide groups are taken into account in the analysis of radionuclide transport and deposition. In particular, volatile radionuclides species, such as iodine and cesium, may be transported in more than one chemical form - each with different properties that affect their transport.

Chemical forms of these radionuclide groups represented in the source term analysis of a full-scope PRA include:

Radionuclide Group	Chemical forms for transport
I	I_2, CH_3I , HI [vapor] CsI [aerosol]
Cs	CsOH, CsI [aerosol]

A second simplification in the characterization of radionuclide release involves the treatment of time-dependence. Temporal variations in radionuclide release are calculated as a natural product of deterministic source term calculations. However, in a Level 2 PRA these variations are reduced to a series of discrete periods of radiological release, each of which is described by a starting time, a duration, a (constant) release rate, and a release energy. For example, results of an integral severe accident/source term code calculation might suggest the radiological release rate shown as the solid line in Figure 3.10. The continuous release rate is simplified to represent major characteristics or the release history such as an early, short-lived, large release rate immediately following containment failure (sometimes referred to as the "puff release"), followed by two longer periods of a sustained release. The specific characteristics of these discrete release periods may vary from one accident sequence (or plant damage state) to another, but the timing characteristics (i.e., start

Table 3-21 Radionuclide grouping scheme used in a Level 2 PRA

Group	Rep. element	Elements represented by the group	Important isotopes within the group
1	Xe	Xe, Kr	Xe-133, Xe-135, Kr-85, Kr-85M, Kr-87, Kr-88
2	I	I, Br	I-131, I-132, I-133, I-134, I-135
3	Cs	Cs, Rb	Cs-134, Cs-136, Cs-137, Rb-86
4	Te	Te, Sb, Se	Te-127, Te-127M, Te-129, Te-129M, Te-131, Te-132, Sb-127, Sb-129
5	Sr	Sr	Sr-89, Sr-90, Sr-91, Sr-92
6	Ru	Ru, Rh, Co, Mo, Tc, Pd	Ru-103, Ru-105, Ru-106, Rh-105, Co-58, Co-60, Mo-99, Tc-99M
7	La	La, Y, Zr*, Nb, Nd, Pr, Am, Mc, Sm	La-140, La-141, La-142, Y-90, Y-91, Y-92, Y-93, Zr-95, Zr-97, Nb-95, Nd-147, Pr-143, Am-241, Cm-242, Cn-244
8	Ce	Ce, Np, Pu	Ce-141, Ce-143, Ce-144, Np-239, Pu-238, Pu-239, Pu-240, Pu-241
9	Ba	Ba	Ba-139, Ba-140

*Radionuclide Zirconium (not the structural metal)

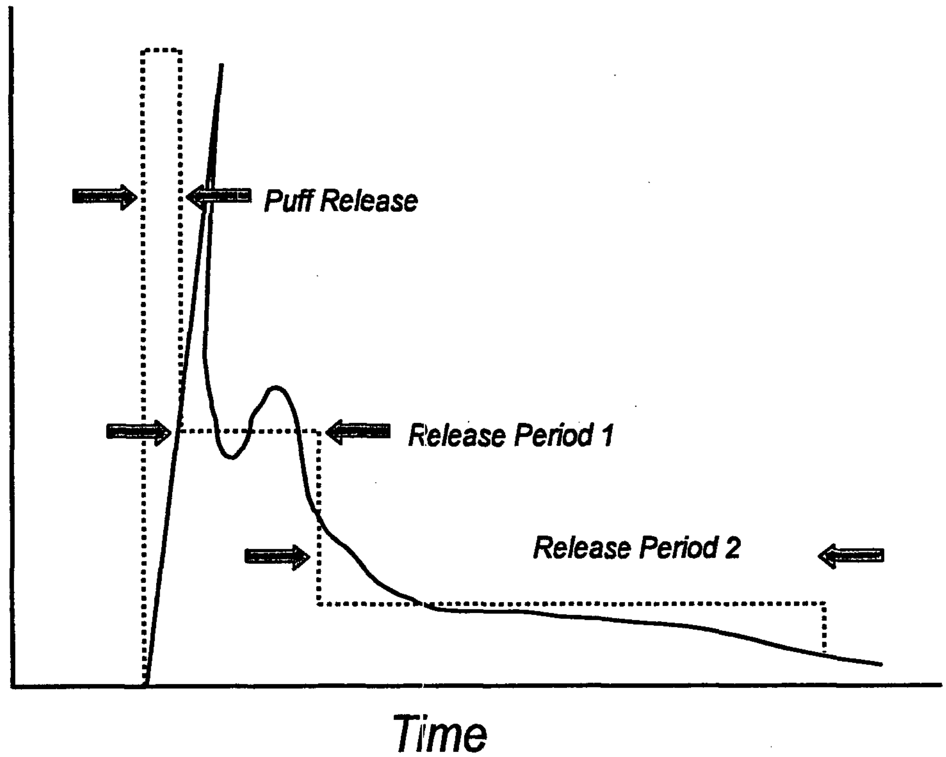

Figure 3.10 Example of simplified radionuclide release rates

time and duration) are the same for each radionuclide group (i.e., only the release rate varies from one group to another for a given release period). The total number of release periods is typically small (i.e., 3 or 4) and represents distinct periods of severe accident progression. For example, the following time periods may be represented:

Very early [containment leakage prior to containment failure]

Puff release [immediately following containment failure]

Early [relatively large release rate period accompanying containment depressurization following breach of the containment pressure boundary]

Late [long-term, low release rate after containment depressurization]

Note that the above time periods are for illustrative purposes only; others are developed, as necessary, to suit the specific results of a plant-specific assessment.

Task 2 – Coupling Source Term and Severe Accident Progression Analyses

The number of unique severe accident sequences represented in a Level 2 PRA can be exceedingly large. Comprehensive, probabilistic consideration of the numerous uncertainties in severe accident progression can easily expand a single accident sequence (or plant damage state) from the Level 1 systems analysis into a large number of alternative severe accident progressions. A radionuclide source term must be estimated for each of these accident progressions. Clearly, it is impractical to perform that many deterministic source term calculations.

A common practice in many Level 2 PRAs (although insufficient for a state-of-the-art PRA) is to reduce the analysis burden by grouping the alternative severe accident progressions into "source term bins" or "release categories." This grouping process is analogous to the one used at the interface between the Level 1 and Level 2 analyses to group accident sequence cut sets into plant damage states. The principal objective of the source term grouping (or binning) exercise is to reduce the number of specific severe accident scenarios for which deterministic source term calculations must be performed to a practical value. A structured process similar to the one described in Section 3.3.1 (related to the assessment of accident sequences addressed in a Level 2 PRA) is typically followed to accomplish the grouping. Characteristics of severe accident behavior and containment performance that have a controlling influence on the magnitude and timing of radionuclide release to the environment are used to group (or bin) the alternative accident progressions into appropriate release categories. A deterministic source term calculation is then performed for a single accident progression within each release category (typically the highest frequency) to represent the entire group.

As indicated above, this approach is inadequate for a state-of-the-art Level 2 analysis because the radionuclide source term for any given severe accident progression cannot be calculated with certainty. The influence of uncertainties related to the myriad processes governing radionuclide release from fuel, transport through the primary coolant system and containment, and deposition on intervening structures is significant and must be quantified with a similar level of rigor afforded to severe accident progression uncertainties. Further, a state-of-the-art Level 2 PRA is performed in a manner that allows the relative contribution of individual parameter uncertainties to the overall uncertainty in risk to be calculated directly (i.e., via rank regression or some other statistically rigorous manner). This requires a probabilistic modeling process that combines the uncertainty distributions associated with the evaluation of accident frequency, severe accident progression, containment performance, and radionuclide source terms in an integrated, consistent fashion.

In performing this integrated uncertainty analysis, special care must be taken to ensure consistency between uncertain parameters associated with radionuclide release, transport, and deposition and other aspects of accident behavior. In particular, the analysis must account for important correlations between the behavior of radionuclides and the other characteristics of severe accident progression. For example;

- The magnitude of radionuclide release from fuel is known to be influenced by the magnitude of Zircaloy (clad) oxidation. Therefore, the distributions of plausible values for the release fraction of various radionuclides are correlated to the distribution of values for the fraction of clad oxidized in-vessel.

- In the NUREG-1150 (NRC, 1990) assessments, uncertainty in the retention efficiency of aerosols transported through the primary coolant system was found to depend strongly on primary coolant system pressure during in-vessel melt progression. Higher retention efficiencies were attributed to sequences involving low coolant system pressure than those involving high pressure.

These and other similar relationships are described in the experts' determination of source term issues in NUREG/CR-4551, Volume 2 (Harper, 1990).

Task 3 – Treatment of Source Term Uncertainties

Results of the Level 2 PRAs described in NUREG-1150 indicate that uncertainties associated with processes governing radionuclide release from fuel; transport through the primary coolant system, secondary coolant system (if applicable), and containment; and deposition on bounding structures can be a major contributor to the uncertainty in some measures of risk. For example, uncertainties in the magnitude of radionuclide release from fuel during in-vessel melt progression, and uncertainties in the amount of retention on the shell (secondary) side of steam generators were found to be among the largest contributors to the overall uncertainty in early fatality risk associated with steam generator tube rupture events (a significant contributor to the core damage frequency in some PWRs). Similarly, uncertainties in processes such as radionuclide release during core-concrete interactions and late release of iodine initially captured by pressure suppression pools were found to be important contributors to various risk measures in BWRs.

Uncertainties in the processes specifically related to radionuclide source term assessment are, therefore, represented in a state-of-the-art Level 2 PRA. When deterministic codes are used to estimate the source term, it is important to account for all of the relevant phenomena (even when the code does not explicitly include models for all of the phenomena). When a model is not available for certain important phenomena, it is not acceptable to simple ignore the phenomena. Instead, alternative methods are used, such as consulting different code calculations, using specialized codes, or assessing relevant experimental results. A systematic process and calculation tools to accommodate source term uncertainties into the overall evaluation of severe accident risks were developed for the Level 2 PRAs described in NUREG-1150. A detailed description of this process and the associated tools is not provided here; the reader is referred to NUREG/CR-4551, Vol. 2, Part 4 (Harper, 1990), NUREG-1335 Appendix A (NRC, 1989), and NUREG/CR-5360 (Jow, 1993), for additional information on these topics. In addition, when estimating consequences in the PRA, it is also important to accurately represent the timing of the release. Past studies have shown that the number of early fatalities can be particularly sensitive to when the release occurs relative to when the general public is being evacuated. Hence, it is also important that the approach used to estimate the source term properly accounts for timing characteristics of the release.

Table 3-22 summarizes the areas in which key uncertainties are addressed in a Level 2 analysis. These key uncertainties are derived, in part, from the results of the NUREG-1150 analyses, as well as more recent statements of key source term uncertainties published by the NRC for light-water reactor licensing purposes.

3.3.5.4 Task Interfaces

These tasks have a critical interface with the containment probabilistic characterization (refer to Task 2 of Section 3.3.4).

The output of these tasks is a range of potential containment failure modes, release fractions (or source terms), and their corresponding frequencies. The output of the Level 2 analysis provides input to the consequence analysis (Section 3.4).

Table 3-22 Areas of key radionuclide source term uncertainties

Magnitude of radionuclide release from fuel during core damage and material relocation in-vessel (primarily for volatile and semi-volatile radionuclide species).
Chemical form of iodine for transport and deposition.
Retention efficiency during transport through the primary and secondary coolant systems (particularly for long release pathways).
Magnitude of radionuclide release from fuel (primarily refractory metals) and non-radioactive aerosol generation during core-concrete interactions.
Decontamination efficiency radionuclide flow streams passing through pools of water (BWR suppression pools and PWR containment sumps).
Late revaporization and release of iodine initially captured in water pools.
Capture and retention efficiency of aerosols in containment and secondary enclosure buildings.

3.3.5.5 References

EPRI, "MAAP4 - Modular Accident Analysis Program for LWR Power Plants," RP3131-02, Volumes 1-4, Electric Power Research Institute, 1994.

Summers, R., M, et al., "MELCOR Computer Code Manuals -- Version 1.8.3," NUREG/CR-6119, SAND93-2185, Volumes 1-2, Sandia National Laboratories, 1994.

NRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, U.S. Nuclear Regulatory Commission, December 1990.

Harper, F. T., et al, "Evaluation of Severe Accident Risks: Quantification of Major Input Parameters," NUREG/CR-4551, Volume 2, SAND86-1309, Sandia National Laboratories, December 1990.

NRC, "Individual Plant Examination: Submittal Guidance," NUREG-1335, U.S. Nuclear Regulatory Commission, August 1989.

Jow, H. J., et al., "XSOR Codes User Manual," NUREG/CR-5360, Sandia National Laboratories, 1993.

3.4 Level 3 Analysis (Consequence Analysis and Integrated Risk Assessment)

In this section, the analyses performed as part of the Level 3 portion of a probabilistic risk assessment (PRA) are described.

3.4.1 Assumptions and Limitations

In most Level 3 (i.e., 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 Organization 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, 1996).

3.4.2 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.

3.4.3 Analytical Tasks

A Level 3 PRA consists of two major tasks:

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.

Task 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, 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.

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, 1990 and Chanin, 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, 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, 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.

To use a 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 area 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.

Task 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.

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.

3.4.4 Task Interfaces

The current task requires a set of release fractions (or source terms) from the Level 2 analysis (Section 3.3) 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. 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.

3.4.5 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 Cooperation and Development, Nuclear Energy Agency, Paris, France, 1994.

3.5 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. 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 section, the way in which a Level 1 PRA is modified in order to model accidents initiated by internal floods is described.

3.5.1 Assumptions and Limitations

When preparing this section, some assumptions and limitations were made as indicated below:

- It is assumed that flood and spray incidence data from WERs 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.

3.5.2 Products

During the conduct of this task, the scenario tables initiated in the Spatial Interactions Task are expanded upon and refined (an example of such a table is provided in Appendix C). The completed and refined scenario tables make up a key product for this effort.

A description of the methodology and the data analyses utilized to perform the flood analysis will be developed.

3.5.3 Analytical Task

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, 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).

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 are accomplished by the performance of five tasks:

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).

Task 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 flood 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.

Task 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. 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.

Task 3 – Performance 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., ½0 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.

Task 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.

Task 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.

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.

3.5.4 Task Interfaces

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 on Spatial Interactions. The conduct of this task will require input from the tasks on Initiating Event Analysis, Frequency of Initiating Events, Event Sequence Modeling, and System Modeling. 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.

Output from the Flood Analysis task provides information on accident sequence definition and on frequency of occurrence directly to the Level 2 task, which in turn provides source term information to the consequence and risk integration task. Whether or not Level 2/3 analyses are performed depends on the scope of the PRA.

3.5.5 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.

3.6 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 sections. 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. In this section, the way in which a Level 1 PRA is modified in order to model accidents initiated by internal fires is described.

3.6.1 Assumptions and Limitations

When preparing this section, some assumptions and limitations were made as indicated below:

1. It is assumed that fire incidence data from WERs 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.

2. 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.

3. 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. A more advanced approach to circuit analysis is provided in LaChance (2003).

4. 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.

5. 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.

3.6.2 Products

During the performance of this task, the scenario tables that were initiated in the Spatial Interactions Task are expanded upon and refined (an example of such a table is provided in Appendix D). The completed and refined scenario tables make up a key product for this effort.

A description of the methodology and the analyses utilized to perform the fire analysis will be developed.

3.6.3 Analytical Tasks

A full power internal fire PRA utilizes the same overall analysis approach and procedures used in performing a full power traditional internal events PRA. 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).

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 activity are accomplished by the performance of five tasks:

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.

Task 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). A tabulation of both U.S. and international fire incidents, including the KNPS Unit 1 fire of 1984, and insights from them are available from Nowlen (2001).

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.

Task 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 3.2.3 (refer to data entry 7 in Table 3-14 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.

Task 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 3-15 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., ½0 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.

Task 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.

Task 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.

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.

3.6.4 Task Interfaces

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. The conduct of this task will require input from the tasks dealing with Initiating Event Analysis, Frequency of Initiating Events, Event Sequence Modeling, and System Modeling. 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.

Output from the Fire Analysis task provides information on accident sequence definition and on frequency of occurrence directly to the Level 2 task which in turn provides source term information to the consequence and risk integration task. Whether or not Level 2/3 analyses are performed depends on the scope of the PRA.

3.6.5 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.

LaChance, J., et al., "Circuit Analysis - Failure Mode and Likelihood Analysis," NUREG/CR-6834, Sandia National Laboratories, September 2003.

Nowlen, et al., "Risk Methods Insights Gained from Fire Incidents," NUREG/CR-6738, U.S. Nuclear Regulatory Commission, September 2001.

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

3.7 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 Section 3.2. 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. In this section, 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.

3.7.1 Assumptions and Limitations

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.

3.7.2 Products

The products of this task include, as a minimum, the development of a seismic hazard curve, a listing of seismically 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 documentation on the following:

1. The seismic hazard curve and its basis.

2. The original equipment and structures list for inclusion in the fragility analysis, and the 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). The fragility curves for plant structures and probabilistic safety assessment-related equipment and the details of the fragility analysis.

3. 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

3.7.3 Analytical Tasks

The scope of the seismic analysis should include:

Task 1 Seismic Hazard Analysis
Task 2 Structures and Component Fragility Analysis
Task 3 Plant Logic Analysis
Task 4 Quantification

Each of these tasks is discussed below. 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 Section 3.2 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.

Task 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, ©) 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 cross-checking, 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).

Task 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.

Task 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 de-energizing 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.

Task 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.

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.

3.7.4 Task Interfaces

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. The conduct of this task will require input from the tasks dealing with Initiating Event Analysis, Frequency of Initiating Events, Event Sequence Modeling, and System Modeling. 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.

Output from the Seismic Analysis task provides information on accident sequence definition and on frequency of occurrence directly to the Level 2 task which in turn provides source term information to the consequence and risk integration task. Whether or not Level 2/3 analyses are performed depends on the scope of the PRA.

3.7.5 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.

4. DOCUMENTATION

This chapter establishes guidance for documenting a PRA. Documentation of the PRA has two major objectives:

- Present the results of the study (i.e., communicate information), and
- Provide traceability of the work.

Documentation begins with 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 Reports for each of the major technical activities of the PRA. All of this documentation is then used to recast the model and results into the Executive Summary. Finally, an Overall Project Summary is developed, which presents key results and insights from the work.

4.1 Documentation in Support of Reporting/Communication

Table 4-1 briefly summarizes the reports used to document the KNPS PRA. The distribution of these reports is also indicated in the table. Each report is discussed in more detail below.

Table 4-1 Documentation for the Kalinin PRA Project

Report	Distribution
Executive Summary Report – Level 1, Internal Events – Level 2, Internal Events – Other Events[1]	NUREG/IA-0212, Volume 1 Publicly Available
Main Report–Level 1 PRA, Internal Initiators **Main Report–Level 2 PRA, Internal Initiators** **Main Report–Other Events Analysis (Fire, Flood, Seismic)**	NUREG/IA-0212, Volume 2, Part 1 NUREG/IA-0212, Volume 2, Part 2 NUREG/IA-0212, Volume 2, Part 3 Proprietary/Restricted Distribution
Procedure Guides for a Probabilistic Risk Assessment	NUREG/CR-6572, Revision 1 Publicly Available

[1]Does not include quantitative results for core damage frequency and radionuclide release frequency

The Procedure Guides for a Probabilistic Risk Assessment report 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 Project/Executive Summary report 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) and a Level 2 PRA (containment performance) were carried out in detail. A Level 3 PRA was not performed but guidance on performing such a PRA was provided.

The Main Report documents the Level 1 PRA performed for accidents initiated by internal events at the KNPS. The report was written by the Russians and contains an explanation of the methods used and the results of the overall analysis as well as the analysis done for the technical activities within the Level 1 PRA.

The Main Report also documents the Level 2 Internal Events PRA. This was also written by the Russians and contains an explanation of the methods used and the results of the overall analysis as well as the analysis done for the technical activities within the Level 2 PRA.

The Main Report also includes a description of the analyses performed for Other Events. The section summarizes the analyses that were performed for accidents initiated by internal floods, fire and seismic events. It was written jointly by the Russian-American team.

The Appendices for the Level 1 and Level 2 Internal Events PRA were written by the Russians and complement the Main Report by providing more details on the Level 1 and Level 2 analyses.

4.2 Documentation in Support of Traceability

Documentation should be performed in such a manner that facilitates applications, updating and peer review of the PRA. This section provides general guidance. Reference should be made to the technical activities described in Chapter 3 for guidance on specific products expected from individual technical activities.

Documentation supporting the PRA technical activities should be legible and retrievable (i.e., traceable). PRA documentation should clearly indicate the owner's approval authorization, as appropriate.

The methodology that was used in performing the technical activities in Chapter 3 should be identified either in owner-specific documents or through reference to existing methodology documents. In addition, any general assumptions, interfaces with other PRA elements, nomenclature, definition of terms, or other specific element items that need to be included should be documented.

Information sources, both plant-specific and generic, used in performing the technical activities should be documented including those sources that are mandatory.

Assumptions and limitations made in performing the technical activities should be documented. including those decisions and judgments that were made in the course of the analysis. The justification should also be included; the justification should provide sufficient detail to allow a reviewer to understand the appropriateness of the assumption or the limitation. General or generic assumptions and limitations should be documented.

The products and outcomes from the technical activities should be documented. These products and outcomes should include those products or deliverables that are necessary to understand the process used to satisfy the technical activities.

The documentation of the technical activities should indicate the person(s) who developed or prepared the product or outcome and the person(s) who reviewed or otherwise verified the appropriateness of the product or outcome with a printed name and associated signature. The person(s) reviewing, verifying, or otherwise checking products and outcomes should not have participated in the preparation of the product or outcome for which they were assigned.

APPENDIX A
RECOMMENDED SUPPLEMENTAL CCF GENERIC ESTIMATES FOR KALININ PRA BASED ON EXPERIENCE IN THE U.S.

This appendix provides information on supplemental common-cause failure (CCF) estimates for some of the instrumentation and control components which are not currently contained in Stromberg et al. (1995). The specific components of concern are:

- Pressure sensors
- Sensors: flux monitors
- Sensors: temperature detectors
- Relays
- Analog channel
- Digital channel.

There is not currently a specific reference addressing the CCF for all of the above components. Several different references were reviewed, and that portion of data which was considered appropriate was used to arrive at the final recommended values. Some references were of a proprietary nature and, therefore, could neither be referenced nor quoted. Such references were used as a check on the final results to ensure that the recommended uncertainty ranges cover the CCF values reported in these proprietary references. The recommended values are provided in the form of the Beta factor for various group sizes. The references that were reviewed for this appendix (excluding the proprietary references) are given below.

A.1 Pressure Sensors

Pressure sensors include both mechanical (spring assisted force balance) and electrical (balanced capacitors) transducers. They can be used for measurements of pressure and pressure differential (delta pressure). The measurements on delta pressure could be indirectly used for level and flow measurements. Different types of pressure sensors used for different applications can have significantly different failure rates. However, the estimated generic CCF parameters do not differentiate between different types and applications. Such generic CCF estimates could be used for the initial phase of quantification. Limited failure data was analyzed in Atwood (1983) for pressure sensors; however, the pressure sensors, their logic channel, relays, and switches were all combined. Another study of pressure transmitters focusing on a specific manufacturer of the electrical type (Carbonado et al., 1991) focuses on specific types of failure mechanisms, i.e., loss of fill oil. Carbonado and Azarm (1993) uses a beta factor of 0.21 for conditional failure probability of at least two pressure transmitters out of a group of three. Other studies of pressure transmitters all indicate that these types of components are typically reliable, fully tested infrequently, and there is a high potential for dependent failures. Based on the review of all the materials, Table A-1 provides the reasonable generic data for use as the prior for pressure transmitters.

Table A-1 Generic CCF rates for pressure transmitters used as pressure, level, or flow monitors

Group Size	2 or More Given 1	3 or More Given 1	4 or More Given 1	Lognormal Error Factor
2	0.15	NA	NA	6
3	0.2	0.1	NA	6
4	0.2	0.1	0.1	6

A.2 Sensors: Flux Monitors

This includes source range monitors (typically proportional counters), intermediate range monitors (typically compensated ionization chambers), and finally, power range monitors (typically uncompensated ionization chambers). Atwood (1983) and Azarm et al. (1989) were reviewed and both indicated that CCF rates for such components are very low. Therefore, it is recommended that a global Beta factor of 0.01 with an error factor of 3 be used for these types of flux monitors.

A.3 Sensors: Temperature Detectors

Atwood (1983) provides the CCF rate for resistance temperature detectors. The majority of failure modes are due either to moisture leakage or high resistance of the resistors. Some drift failures were also reported. The reasonable values provided in Table A-2 are primarily based on the actual event data reported in Atwood (1983) with the exception of error factors which are subjectively assigned.

A.4 Relays

A global Beta factor of 0.07 is reported for relays in Hassan and Vesely (1997). Similarly, Martinez-Garret and Azarm (1994) report a global Beta factor of 0.06 with an error factor of 2.2 for relays based on actuarial data of onsite electrical power system in U.S. nuclear power plants. The use of a global error factor is justified since the level of redundancy in most cases was 2. Both studies do not differentiate between different types and applications of relays (e.g., master vs. slave) for CCF rates. Azarm et al. (1994) focuses on the specific relay manufacturer and indirectly provides a global Beta factor by determining the "F" factor. In Azarm et al. (1994), (1/F) is the ratio of the actual system unavailability accounting for independent plus dependent contributions divided by the independent portion. This study considers that CCFs of the relays are due mainly to slow acting CCF mechanisms, such as insulation wear-out and varnish deposition on the relay contacts. These global Beta factors, therefore, are sensitive to test intervals; a short test interval will detect individual failures before becoming multiple failures. For a test interval of about one year, a global Beta factor of about 0.06 for a group size of 2, and a global Beta factor of 0.02 for group sizes of three or more is estimated. It is important to note that increasing the test interval by a factor of 2 could double the values of the beta factors estimated. Therefore, we recommend a Beta factor of 0.06 with an error factor of 2.2 for a group size of 2 and a Beta factor of 0.02 with an error factor of 3 for a group size of three or more with earlier adjustment of a test interval if it exceeds one year.

Table A-2 Generic CCF rates for resistance temperature detectors excluding the in-core thermocouples

Group Size	2 or More Given 1	3 or More Given 1	4 or More Given 1	Lognormal Error Factor
2	0.14	NA	NA	6
3	0.14	0.07	NA	6
4	0.2	0.1	0.07	6

A.5 Analog Channel

An analog channel is typically responsible for signal conditioning by methods, such as modulation, de-modulation, filtering, or amplifying. The last stage of an analog channel is either a driver amplifier to feed a device or a relay, or a comparator to provide input to a logic channel. Solid-state analog circuits have been in use for many years, and there is good understanding of their failure mechanisms. CCF of analog circuits due to heat, humidity, electrical surges, lightening, smoke, and vibration have been observed in the past. The CCF rates for analog channels are application dependent; however, Hassan and Vesely (1997) and Azarm et al. (1989) provide some generic CCF rates for the analog channels, i.e., 0.07 from Hassan and Vesely (1997) and 0.05 from Azarm et al. (1989). Primarily based on these references, a global Beta factor of 0.07 should be used for analog channels (regardless of group size). An error factor of 6 is recommended to indicate the variation of this global beta factor with the specific application type.

A.6 Digital Channels

A digital channel could be a programmable logic module, a logic circuitry, a processor unit with the associated memory and bus structure, etc. The components in a digital channel could be made using a variety of different semiconductor technologies. The CCF associated with these components are mostly driven by external causes; therefore, they should operate in a controlled environment. A global Beta factor of 0.001 is reported for logic modules in Hassan and Vesely (1997). An error factor of 10 to indicate the significant variability and uncertainty in this CCF estimate is recommended.

A.7 References

Atwood, C. L., "Common-Cause Fault Rates for Instrumentation and Control Assemblies," NUREG/CR-2771, Idaho National Engineering Laboratory, February 1983.

Azarm, M. A., et al., "Dependent Failures and Two Case Studies," BNL Technical Report W6082, Brookhaven National Laboratory, August 1994.

Azarm, M. A., et al., "Level 1 Internal Event PRA for the High Flux Beam Reactor," BNL Technical Report, Brookhaven National Laboratory, August 1989.

Carbonado, J., and M. A. Azarm, "Evaluation of Surveillance and Technical Issues Regarding ATWS Mitigation Systems," BNL Technical Report L-1311, Brookhaven National Laboratory, June 18, 1993.

Carbonado, J., et al., "Evaluation of Surveillance and Technical Issues Regarding Rosemount Pressure Transmitter Loss of Fill-Oil Failures," BNL Technical Report L-1311, Brookhaven National Laboratory, December 1991.

Hassan, M., and W. E. Vesely, "Digital I&C Systems in Nuclear Power Plants: Risk Screening of Environmental Stressors and a Comparison of Hardware Unavailability with Existing Analog System," NUREG/CR-6579, November 1997.

Martinez-Garret, G., and M. A. Azarm, " Reliability Assessment of Electrical Power Supply to Onsite Class 1E Buses at Nuclear Power Plants, BNL Technical Report I-2505, Brookhaven National Laboratory, June 7, 1994.

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.

APPENDIX B
SIMPLIFIED LEVEL 2 ANALYSIS

B.1 Background

In this appendix, the analyses performed as part of the Level 2 portion of a probabilistic risk assessment (PRA) are described. The analyses described in this appendix were previously published in an earlier version of this procedure guides (NUREG/CR-6572, Vol. 3, Part 1, September 1999). The approach described is a simplified Level 2 PRA and is included here for completeness. The approach described in the main body of revised procedure guide is a full-scope Level 2 PRA.

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.

B.2 Task Activities

The purpose of this appendix 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 appendix describes six major procedural activities for assessment and management of severe accident risks (see Figure B.1). Section B.2.1 provides guidance on development of plant damage states (PDSs) (Activity 1). Section B.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 B.2.3 discusses the accident progression grouping (source term categorization, Activity 4). Section B.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). Section B.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). Attachment 1 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.

B.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

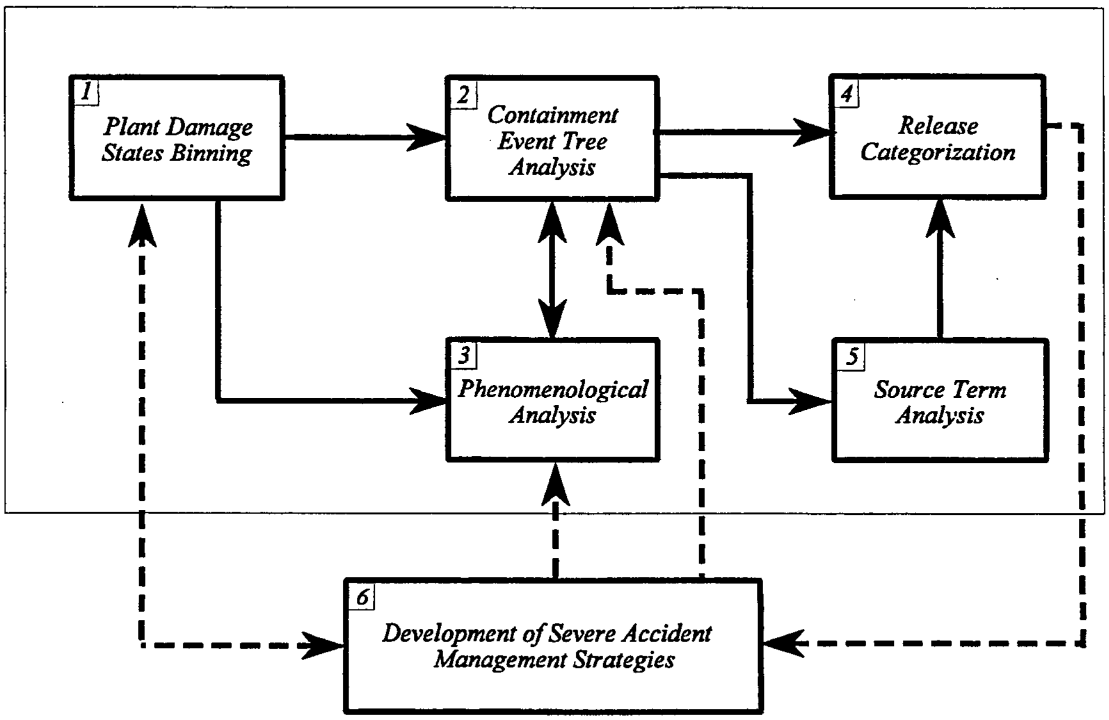

Figure B.1 Major procedural activities for assessment and management of severe accident risks

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 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 B-1 that will identify those accidents that are more challenging to containment integrity than others. The attributes given in Table B-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 B.2.2. The WER analysts should verify that the attributes given in Table B-1 are appropriate and ask themselves whether WERs have some other features that also belong on this table. It should also be noted that the PDS groups in Table B-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 B-1 should be expanded accordingly.

B.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 Attachment 1. The discussion in Attachment 1 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. Attachment 1 lists some of the considerations that need to be addressed by the WER 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 Attachment 1 can be summarized by using event sequence diagrams such as those shown in Figures B.2 and B.3.

Table B-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

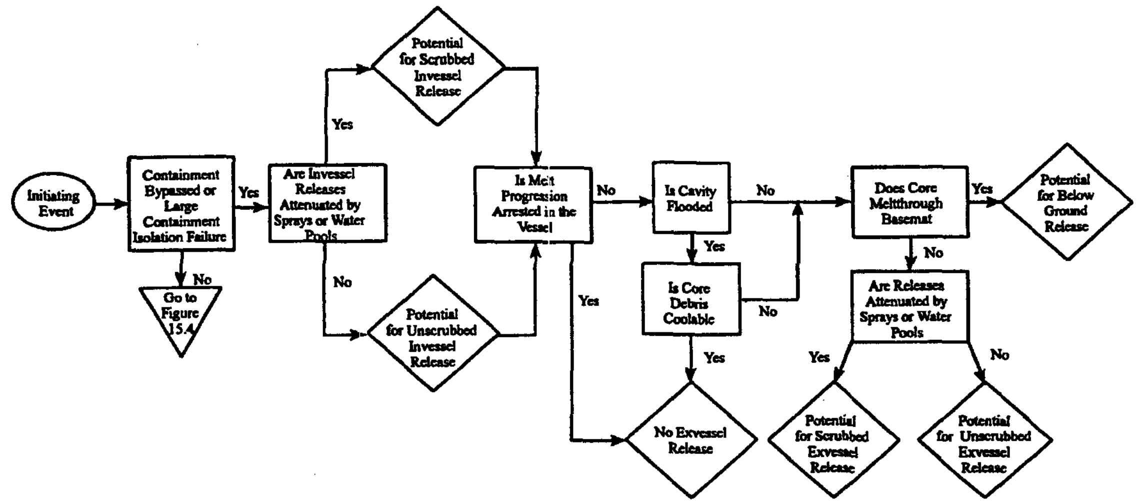

Figure B.2 Event sequence diagram for accidents in which the containment is bypassed or not isolated

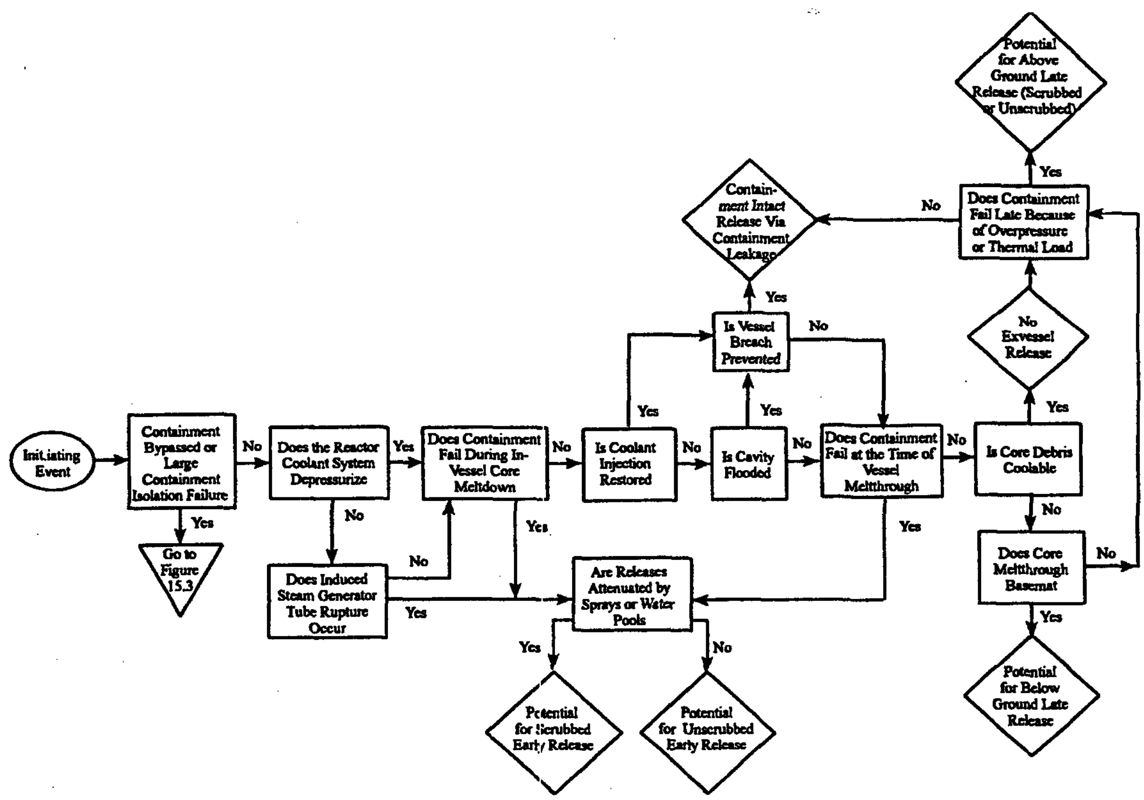

Figure B.3 Event sequence diagram for accidents in which the containment is initially intact

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 B.2), 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.

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 B.3) 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 Attachment 1 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.

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 B.2 and B.3 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 B.2.1. This step is normally achieved by using event trees that incorporate events such as those shown in Figures B.2 and B.3 and address the issues discussed in Attachment 1. 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 B-2.

This CET is based on the event sequence diagrams in Figures B.2 and B.3 and also incorporates the issues discussed in Attachment 1. 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 D-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 Attachment 1). 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 B-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 Attachment 1) 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 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 B.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

Table B-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

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 B.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, Attachment 1 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 B.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 B.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 B.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 B.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 B.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. Attachment 1 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 B.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.

B.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.

B.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 B.2.3) can be obtained.

B.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 B.2.1 through B.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 B.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 B.2.2 (refer to Table B-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).

B.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 B.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.

B.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.

B.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.

B.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.

B.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.

B.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.

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.

ATTACHMENT 1
GUIDANCE ON THE EXAMINATION OF CONTAINMENT SYSTEM PERFORMANCE

INTRODUCTION

This appendix discusses 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. In addition, general guidance on the evaluation of containment system performance given the present state of the art of analysis of these phenomena is provided. The evaluation should be a pragmatic exploitation of the present containment capability. It should give an understanding and appreciation of severe accident behavior, should recognize the role of mitigating systems, and should ultimately result in the development of accident management procedures that could both prevent and ameliorate the consequences of some of the more probable severe accident sequences involved. The information provided here summarizes some more recent developments in core melt phenomenology relevant to containment performance, identifies areas of uncertainty, and suggests ways of proceeding with the evaluation of containment performance despite uncertainties, and potential ways of improving containment performance for severe accident challenges.

The systems analysis portion of the probabilistic risk assessment (PRA) identifies accident sequences that occur as a result of an initiating event followed by failure of various systems or failure of plant personnel to respond correctly to the accident. Although the number of possible core melt accident sequences is very large, the number of containment system performance analyses does not have to be as large. The number of sequences can be reduced by grouping those accident sequences that have a similar effect on the plant features that determine the release and transport of fission products.

STATUS OF CONTAINMENT SYSTEMS PRIOR TO VESSEL FAILURE

In order to examine the containment performance, the status of the containment systems and related equipment prior to core melt should be determined. This requires analyses of (1) the pathways that could significantly contribute to containment-isolation failure, (2) the signals required to automatically isolate the penetration, (3) the potential for generating the signals for all initiating events, (4) the examination of the testing and maintenance procedures, and (5) the quantification of each containment-isolation failure mode (including common mode failures).

In the early phase of an accident, steam and combustible gases are the main contributors to containment pressurization. The objective of the containment decay heat removal systems, such as sprays, fan cooler, and the suppression systems, is to control the evolution of accidents that would otherwise lead to containment failure and the release of fission products to the environs. The effectiveness of the several containment decay heat removal systems for accomplishing the intended mitigating function should be examined to determine the probability of successful performance under accident conditions. This includes potential intersystem dependencies as well as the identification of all the specific functions being performed and the determination of the mission time considering potential failure due to inventory depletion (coolant, control air, and control power) or environmental conditions. If, as a result of the accident sequence, the frontline containment decay heat removal systems fail to function, if their effectiveness is degraded, or if the operator fails to respond in a timely manner to the accident symptoms, the containment pressure would continue to increase. In this case, some systems that were not intended to perform a safety function might be called upon to perform that role during an accident. If the use of such systems is considered during the examination, their effectiveness and probability of success for fulfilling the needed safety function should also be examined. Part of the examination should be to determine if adequate procedures exist to ensure the effective implementation of the appropriate operator actions.

PHENOMENA AFTER VESSEL FAILURE

If adequate heat removal capability does not exist in a particular accident sequence, the core will degraded and the containment could potentially overpressurize and eventually fail. Efforts to stabilize the core before reactor vessel failure or to extend the time available for vessel reflood should be investigated. For certain accident groups that proceed past vessel failure, the containment pressurization rate could exceed the capability of the mitigating systems to reject the energy associated with the severe accident phenomena encountered with vessel failure. For each such accident sequence, the molten core debris will relocate, melting through and mixing with materials in its path. Depending on the particular containment geometry and the accident sequence groups, a variety of important phenomena influence the challenges to containment integrity.

The guidance provided below deals with this subject at three levels. The first provides some rather general considerations regarding the nature of these phenomena as they impact containment. The second level considers the manifestation of these phenomena in more detail within the generic high and low pressure scenarios. Finally, the third level provides some specific guidance particularly regarding the treatment of certain important areas of uncertainty.

General Description of the Phenomena Associated with Severe Accident Considerations

The contact of molten corium with water, referred to as fuel-coolant interaction, can occur both in-vessel and ex-vessel. If the interaction is energetic inside the reactor vessel, it may generate missiles and a rapid pressurization (steam explosion) of the primary system. Early containment failure associated with in-vessel steam explosions (alpha mode failure) is generally considered to be of low enough likelihood to not warrant additional consideration (Basu and Ginsberg, 1996). However, smaller, less energetic in-vessel steam explosions are not unlikely and their influence on fission product release and hydrogen generation are still under investigation. If the fuel-coolant interaction occurs ex-vessel, as might happen if molten fuel fell into a water-filled cavity upon vessel meltthrough, it may disperse the corium and lead to rapid pressurization (steam spike) of the containment. In any case, at one extreme, abundant presence of water would favor quenching of the corium mass and the continued dissipation of the decay heat by steaming would lead to containment pressurization. Clearly in the absence of external cooling, the containment will eventually overpressurize and fail, although the presence of extensive, passive heat sinks (structures) within the containment volume would delay the occurrence of such an event. Fuel-coolant interactions can also yield a chemical reaction between steam and the metallic component of the melt, producing hydrogen and the consequent potential for burns and/or explosions.

At the other extreme, when water is not available, the principal interaction of the molten corium is with the concrete floor of the containment. This interaction produces three challenges to containment integrity. First, the concrete decomposition gives off noncondensible gases (CO_2, CO) that contribute to pressurizing the containment atmosphere. Second, concrete of certain compositions decomposes and releases CO_2 and steam, which can interact with the metallic components in the melt to yield highly flammable CO and H_2, with potential consequences ranging from benign burns at relatively low hydrogen concentrations to rapid deflagrations at high hydrogen concentrations. Third, continued penetration of the floor can directly breach the containment boundary. Also, thermal attack by the molten corium of retaining sidewalls could produce structural failure within the containment causing damage to vital systems and perhaps to failure of containment boundary.

Another type of fuel interaction is with the containment atmosphere. Scenarios can be postulated (e.g., station blackout) in which the reactor vessel and primary system remain at high pressure as the core is melting and relocating to the bottom of the vessel. Continued attack of the molten corium on the vessel lower head could eventually cause the lower head to fail. Because of a potentially high driving pressure, the molten corium could be energetically ejected from the vessel. Uncertainties remain related to the effect of the following on direct containment heating: (1) vessel failure area, (2) the amount of molten corium in the lower head at the time of failure, (3) the degree to which it fragments upon ejection, (4) the degree and extent to which a path from the lower cavity to the upper containment atmosphere is obstructed, (5) the fragmented molten corium that could enter and interact with the upper containment atmosphere, and (6) cavity gas temperature. Since the containment atmosphere has small heat capacity, the energy in the fragmented corium could rapidly transfer to the containment atmosphere, causing a rapid pressurization. The severity of such an event could be further exacerbated by any hydrogen that may be simultaneously dispersed and direct oxidation (exothermic) of any metallic components. Depending upon this and the other factors previously mentioned, this pressurization could challenge containment integrity early in the event.

Even with the above limited perspective, it should be clear that given a core melt accident, a great deal of the phenomenological progression hinges upon water availability and the outcome of the fuel-coolant interactions; specifically whether a full quench has been achieved and whether the resulting particulates will remain coolable. In general, the presence of fine particulates to any significant degree would imply the occurrence of energetic steam explosions and hence the presence of significant forces that would be expected to disperse the particulates to coolable configurations outside the reactor cavity. Otherwise, the coolability of deep corium beds of coarse particulates is the major concern. A summary of how these mechanisms interface and interact as they integrate into an accident sequence is given below.

Accident Sequences: High-Pressure Scenario

The core melt sequence at high primary system pressure is often due to a station blackout sequence. The high-pressure scenario also represents one of the most significant contributors to risk. The initial stages of core degradation involve coolant boiloff and core heatup in a steam environment. At such high pressures, the volumetric heat capacity of steam is a significant fraction of that of water (about one third), and one should expect significant core (decay) energy redistribution due to natural circulation loops set up between the core and the remaining cooler components of the primary system. As a result of this energy redistribution, the primary system pressure boundary could fail prior to the occurrence of large-scale core melt. The location and the size of failure, however, remain uncertain. For example, concerns have been raised about the possibility of steam generator tube failures and associated containment bypass. If the vessel lower head fails, violent melt ejection could produce large-scale dispersal and the direct containment heating phenomenon mentioned previously.

Concerns may also be raised about the potentially energetic role of hydrogen within the blowdown process. The presence of hydrogen arises from two complementary mechanisms: (1) the metal-water reaction occurring at an accelerated pace throughout the in-vessel core heatup/meltdown/slump portion of the transient and (2) the reaction between any remaining metallic components in the melt and the high-speed steam flow that partly overlaps and follows the melt ejection from the reactor vessel. The combined result is the release of rather large quantities of hydrogen into the containment volume within a short time period (a few tens of seconds). The implication is that the consideration of containment atmosphere compositions and associated burning, explosion, or detonation potential becomes complicated by a whole range of highly transient regimes and large spatial gradients.

The NUREG-1150 severe accident risk study (NRC, 1990) was the first systematic attempt to treat direct containment heating (DCH) from a

PRA perspective by integrating sequence probabilities with uncertainties associated with initial/boundary conditions and phenomenological uncertainties associated with predicting containment loads.

Since the completion of the NUREG-1150 study, advances have been made in the ability to predict the probability of containment failure by DCH in pressurized water reactors. The U.S. Nuclear Regulatory Commission has identified DCH as a major issue for resolution in the Revised Severe Accident Research plan and has sponsored analytical and experimental programs for understanding the key physical processes in DCH. An extensive database resulted from scaled counterpart experiments conducted by Sandia National Laboratory and Argonne National Laboratory. This database has allowed the development and validation of simple analytical models for predicting the containment loads. In particular, a two-cell equilibrium model was developed based on insight from the experimental program and has been used in the DCH issue resolution process. The two-cell equilibrium model takes into account the coherence between the entrained debris and the reactor coolant system blowdown steam.

The results of a probability assessment of DCH-induced containment failure for the Zion Nuclear Power Plant were published in NUREG/CR-6075 and its supplement (Pilch, Yan, and Theofanous, 1994). NUREG/CR-6338 (Pilch et al., 1996) used the methodology and scenarios described in NUREG/CR-6075 to address the DCH issue for all Westinghouse plants with large volume containments, including 34 plants with large dry containments and 7 plants with subatmospheric containments. DCH loads versus strength evaluation were performed in a consistent manner for all plants. The phenomenological modeling was closely tied to the experimental database. Plant-specific analyses were performed, but sequence uncertainties were enveloped by a small number of splinter scenarios without assignment of probabilities. The results of screening calculations reported in NUREG/CR-6338 indicate that only one plant showed a containment conditional failure probability based on the mean fragility curves greater than 0.001. The containment conditional failure probability for this one plant was found to be less that 0.01.

Accident Sequences: Low-Pressure Scenario

At low system pressure, decay heat redistribution due to natural circulation flow (in steam) is negligible and core degradation occurs at nearly adiabatic conditions. Steam boiloff, together with any hydrogen generation, is continuously released to the containment atmosphere, where mixing is driven by natural convection currents coupled with condensation processes. The upper internals of the reactor vessel remain relatively cold, offering the possibility of trapping fission product vapor and aerosols before they are released to the containment atmosphere. Throughout this core heatup and meltdown process, the potential to significantly load the containment is small. The first possibility for significant energetic loads on the containment occurs when the molten core debris penetrates the lower core support structure and slumps into the lower plenum. The outcome of this interaction cannot be predicted precisely. Thus, a whole range of behavior must be considered in order to cover subsequent events. At the one extreme, the interaction is benign, yielding no more than some steam (and hydrogen) production while the melt quickly reagglomerates on the lower reactor vessel head. At the other extreme, an energetic steam explosion occurs. It may be possible to distinguish intermediate outcomes by the degree to which the vessel integrity is degraded. In analyzing this phase of the accident scenario, the important tasks are to determine the likelihood of containment failure and to define an envelope of corium relocation paths into the containment. The latter is needed to ensure the assessment of the potential for such a phenomenon as liner meltthrough.

Consideration should also be given to ex-vessel coolability as the corium can potentially interact with the concrete. The non-energetic release (vessel lower head meltthrough) and spreading upon the accessible portions of the containment floor below the vessel needs to be examined. There is a great deal of variability in accessible floor area among the various designs for some pressurized water reactor cavity designs. The area over which the core debris could spread is rather small given whole-core melts and the resultant pool being in excess of 50 cm deep. In the absence of water, all these configurations would yield concrete attack and decomposition of variable intensity. In the presence of water (i.e., containment sprays), even deep pools may be considered quenchable and coolable. However, the possibility exists for insulating crusts of vapor barriers at the corium-water interface.

Both of these two extremes should be considered. The task is to estimate the range of containment internal pressures, temperatures, and gas compositions as well as the extent of concrete floor penetration and structural attack until the situation has been stabilized. In general, pressurization from continuing core-concrete interactions (dry case) would be considerably slower than from coolable debris configurations (wet case) because of the absence of steam pressurization.

As a final and crucial part of this scenario, one must address the combustible gas effect. This must include evaluation of the quantities and composition of combustible gases released to the containment, local inerting and deinerting by steam and CO_2, as well as hydrogen mixing and transport. Also included should be consideration of gaseous pathways between the cavity and upper containment volume to confirm the adequacy of communication to support natural circulation and recombination of combustible gases in the reactor cavity.

GENERAL GUIDANCE ON CONTAINMENT PERFORMANCE

In the approach outlined in this appendix, emphasis is placed on those areas that would ensure that the PRA process considers the full range of severe accidents. The PRA process should be directed toward developing a plant-specific accident management scheme to deal with the probable causes of poor containment performance. To achieve these goals, it is of vital importance to understand how reliable each of the containment event tree estimates are, and what the driving factors are. Decisions on potential improvements should be made only after appropriately considering the sources of uncertainties. Of course, preventing failure altogether is predicated upon recovering some containment heat removal capability. Given that in either case pressurization develops on the time scale of many hours, feasible recovery actions could be planned as part of accident management.

The bulk of phenomenological uncertainties affecting containment response is associated with the high-pressure scenarios. Unless it can be demonstrated that the primary system can be reliably depressurized, a low probability of early containment failure should not be automatically assumed.

Low-pressure sequences, by comparison, present few remaining areas of controversy. These areas include the coolability behavior of deep molten corium pools and the behavior of hydrogen (and other combustibles) in the containment atmosphere. The views and guidance concerning each one of these areas is briefly summarized below.

The concerns about deep corium pools arose from experiments with top-flooded melts that exhibited crust formation and long-term isolation of the melt from the water coolant. Such noncoolable configurations would yield continuing concrete attack and a containment loading behavior significantly different from coolable ones. On the other hand, it has been pointed out that small-scale experiments would unrealistically not favor coolability. This is an area of uncertainty and it is recommended that assessments be based on available cavity (spread) area and an assumed maximum coolable depth of 25 cm. For depths in excess of 25 cm, both the coolable and noncoolable outcomes should be considered. Along these lines, the PRA should document the geometric details of cavity configuration and flow paths out of the cavity, including any water drain areas into it as appropriate.

With respect to hydrogen, the concerns are related to completeness of the current understanding of hydrogen mixing and transport. In general, combustibles accumulate very slowly and only if continuing concrete attack is postulated. For the larger dry containments, because of the large containment volume and slow release rates, compositions in the detonable range may not develop unless significant spatial concentrations exist or significant steam condensation occurs. In general, the containment atmosphere under such conditions would exhibit strong natural circulation currents that would tend to counteract any tendence to stratify. However, condensation-driven circulation patterns and other potential stratification mechanisms could limit the extent of the containment volume participating in the mixing process. For these plants with igniters, the buildup of combustibles from continuing corium-concrete interactions could be limited by local ignition and burning. However, oxygen availability as determined from natural circulation flows could limit the effectiveness of this mechanism. It is recommended that, as part of the PRA, all geometric details impacting the above phenomena (i.e., heat sink distribution, circulation paths, ignition sources, water availability, and gravity drain paths) be documented in a readily comprehensive form, together with representative combustible source transients.

Finally, uncertainties arise for all plants because of lack of knowledge on how the corium will spread following discharge from the reactor vessel. The reactor cavity configuration will influence the potential for direct attack of the liner by dispersed debris, as well as the potential for basemat failure or structural failure due to thermal attack. The staff recommends that the PRA document describe the detailed geometry (including curbs and standoffs) of the drywell floor.

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.

NRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, U.S. Nuclear Regulatory Commission, December 1990.

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.

APPENDIX C
EXAMPLE CONSIDERATION OF A FLOOD SCENARIO IN A PRA

An example of the analysis of a typical flood scenario is given for further guidance. This example gives some indication of the process required to construct detailed flood scenarios for initial refinement.

In one recent probabilistic risk assessment (PRA), an internal flooding scenario, designated FLOODB, was defined to bound the frequency and impacts from potential flooding events in the annulus. This flooding scenario was retained after the original screening evaluations.

The annulus contains relatively large, open, interconnected floor areas at the lowest level, Elevation-6.0 m. All elevations in the annulus are also interconnected through open stairwells and floor grating. Therefore, it was concluded that only one water source presents a significant hazard for submerging PRA equipment that is located at Elevation-6.0 m. Scenario FLOODB accounts for floods that originate from the nuclear service water (VE) connections to the nuclear component cooling water (TF) heat exchangers. It was conservatively assumed for the screening analysis that a flood from any one of the three heat exchangers would be of sufficient size and would continue long enough to submerge all equipment at Elevation-6.0 m.

Each TF heat exchanger is enclosed in a watertight vault sealed by a normally closed door. Therefore, in addition to evaluating the frequency of events that could cause significant flooding from the VE system, the analysis for scenario FLOODB also accounts for coincident failure of these barriers.

Examination of the event summaries in the flood database reveals that a number of flooding events in the generic database have involved personnel errors during testing and maintenance activities. Therefore, the analysis for scenario FLOODB evaluated two major contributions to the flooding event frequency:

$$\varphi_F = \varphi_{F,M} + \varphi_{F,O}$$

where

φ_F = total frequency of flooding events for scenario FLOODB

$\varphi_{F,M}$ = frequency of flooding events that may occur during maintenance activities

$\varphi_{F,O}$ = frequency of flooding events that may occur at other times.

C.1 Maintenance Events

The frequency of maintenance-related flooding events was evaluated by the following expression:

$$\varphi_{F,M} = 3 * [\lambda_m f_d (T/2)(\varphi_{SW}/3) + \lambda_m (8{,}760) f_f f_c + \lambda_m d_m (\varphi_{SW}/3) f_c]$$

where

λ_m = frequency of TF heat exchanger maintenance (maintenance events per hour)

f_d = likelihood that personnel fail to restore the heat exchanger vault to normal conditions after maintenance has been completed; e.g., failure to reclose the door (error per maintenance event)

T = time interval between routine annulus inspections (hours)

φ_{SW} = frequency of Other Service Water System-Related Flooding Events (flooding events per plant year)

f_f = fraction of maintenance events that lead directly to inadvertent loss of system integrity (flooding events per maintenance event)

f_c = likelihood that personnel fail to stop the flood before equipment is damaged, e.g., failure to turn off the VE pumps or close the vault door (error per flooding event)

d_m = mean duration of TF heat exchanger maintenance (hours per maintenance event).

The expression contains an overall multiplication factor of 3 because the terms inside the brackets evaluate the total maintenance-related flooding frequency for only one heat exchanger vault.

The first term in the expression accounts for a condition in which maintenance has been performed in one of the heat exchanger vaults (λ_m). However, personnel may fail to secure the watertight door properly after the maintenance work has been completed (f_d). A flood will occur if the VE connection fails ($\varphi_{sw}/3$) before the operators discover the open door during their routine inspections (T/2). The fraction (T/2) in this term accounts for the fact that the average exposure period for this condition is one-half the annulus routine inspection interval. The fraction ($\varphi_{sw}/3$) accounts for the fact that approximately one-third of the total frequency for Other Service Water System-Related Flooding Events from the database is allocated to each of the three TF heat exchanger vaults.

The second term in the expression accounts for a condition in which maintenance is performed in one of the heat exchanger vaults (λ_m). However, personnel errors during the maintenance work cause a flood from the VE system (f_f). Maintenance and operations personnel fail to stop the flood before the PRA equipment is submerged (f_c). The multiplication factor of 8,760 in this term converts the hourly frequency of TF heat exchanger maintenance into an equivalent annual frequency.

The third term in the expression accounts for a condition in which maintenance is performed in one of the heat exchanger vaults (λ_m). A flood will occur if the VE connection fails ($\varphi_{sw}/3$) during the maintenance interval while the watertight door is open (d_m). Maintenance and operations personnel fail to stop the flood before the PRA equipment is submerged (f_c). The fraction ($\varphi_{sw}/3$) in this term accounts for the fact that approximately one-third of the total frequency for Other Service Water System-Related Flooding Events in the flood database is allocated to each of the three TF heat exchanger vaults.

The following numerical values were used in this analysis:

- Frequency of TF Heat Exchanger Maintenance (λ_m). The mean frequency of TF heat exchanger maintenance from the plant-specific PRA database is 3.91 x 10^{-5} maintenance event per heat exchanger hour.

- Failure to Reclose Watertight Door (f_d). A nominal value of 5 x 10^{-3} error per maintenance event is used for this error rate. This value is based on generic human error rates that are typically applied for failures to restore equipment to the proper configuration after testing or maintenance activities.

- Annulus Inspection Interval (T). It is assumed for this analysis that a routine inspection of the annulus is performed at least once each shift and that the open door would be discovered during this inspection. Therefore, the average time interval between inspections is eight hours.

- Frequency of Service Water Flooding Events (φ_{SW}). The database shows that the mean frequency of Other Service Water System-Related Events is 3.81 x 10^{-3} flooding event per plant year. The data analysis portion of the PRA documents that all of this frequency was conservatively allocated to the TF heat exchanger vaults in the annulus.

- Fraction of Maintenance Events that Involve Floods (f_f). The flooding events' database used contains one event related directly to errors during heat exchanger maintenance. The database includes experience from a total of 740 plant years of operation through July 1987. The generic mean frequency of heat exchanger maintenance from Module VI is approximately 4.15 x 10^{-5} maintenance event per heat exchanger hour. It is conservatively assumed that each plant in the flooding events' database contains only two heat exchangers. Therefore, the total number of heat exchanger maintenance events in 740 plant years is approximately:

  2*(4.15 x 10^{-5})*(8,760)*(740) = 538 maintenance events

  Thus, an approximate estimate for variable f_f is 1/538 floods per heat exchanger maintenance event. However, there is substantial uncertainty about this estimate. Therefore, a lognormal probability distribution was created to represent this conditional frequency, using a median value of 2×10^{-3} and a range factor of 10. The resulting mean value for f_f is 5.33×10^{-3} flood per heat exchanger maintenance event.

- Failure to Stop the Flood before Damage Occurs (f_c). If a flood begins while personnel are in the heat exchanger vault, there are several opportunities to stop the flow before the annulus is flooded to a depth that will submerge the PRA equipment. For example, local personnel may call the control room and request that the appropriate VE pumps be stopped. Local personnel may also try to close the watertight doors to contain the flood water inside the vault. It is very unlikely that no attempts would be made to alert the control room or to stop the flood locally if personnel were in the area and were physically able to respond. A lognormal probability distribution was created to account for a variety of possible conditions that could delay response until the PRA equipment is submerged. This distribution accounts generally for such factors as extremely severe floods that incapacitate all personnel in the vault, unexpected communication delays, failure of independent indications in the control room, etc. A median value of 1×10^{-3} and a range factor of 10 were assigned to account subjectively for these possible conditions. In other words, it was assumed that approximately one flood in one thousand events would be severe enough to disable the local personnel and would continue long enough to submerge the PRA equipment before it is discovered and controlled. The mean value for f_c from this distribution is 2.66×10^{-3} failures per flooding event.

- Mean Duration of TF Heat Exchanger Maintenance (d_m). The mean duration of TF heat exchanger maintenance from the plant-specific PRA database is 108 hours per maintenance event.

These values were used to estimate the following contributions from each of the three maintenance conditions:

$\lambda_m f_d(T/2)(\varphi_{SW}/3) = 9.93 \times 10^{-10}$ flood per year

$\lambda_m(8{,}760)f_f f_c = 4.86 \times 10^{-6}$ flood per year

$\lambda_m d_m(\varphi_{SW}/3)f_c = 1.43 \times 10^{-8}$ flood per year

The total frequency of heat exchanger maintenance-related flooding events is three times the sum of these contributions for each heat exchanger:

$\varphi_{F,M}$ = 1.46×10^{-5} flood per year

C.2 Events Not Related to Maintenance

The frequency of flooding events that are not related to heat exchanger maintenance activities was evaluated by the following expression:

$$\varphi_{F,0} = \varphi_{SW} f_v + \lambda_v(T/2)\varphi_{SW}$$

where

φ_{SW} = frequency of Other Service Water System-Related Flooding Events (flooding events per plant year)

f_v = likelihood that a closed vault door fails when a flood occurs inside the vault (failures per flooding event)

λ_v = frequency that a heat exchanger vault door is opened and left open during normal plant operation (errors per hour)

T = time interval between routine annulus inspections (hours).

The first term in the expression accounts for a condition in which the VE connection fails in one of the three heat exchanger vaults (φ_{sw}). The heat exchanger vault door is closed when the flood occurs, but it fails (f_v).

The second term in the expression accounts for a condition in which personnel have opened one of the heat exchanger vault doors and have inadvertently left it open (λ_v). A flood will occur if the VE connection fails (φ_{sw}) before the operators discover the open door during their routine inspections (T/2). The fraction (T/2) in this term accounts for the fact that the average exposure period for this condition is one-half the annulus routine inspection interval.

The following numerical values were used in this analysis:

- Frequency of Service Water Flooding Events (φ_{sw}). The plant-specific database shows that the mean frequency of Other Service Water System-Related Events is 3.81×10^{-3} flooding event per plant year. The database documentation also indicates that all of this frequency was conservatively allocated to the TF heat exchanger vaults in the annulus.

- Failure of Closed Watertight Door (f_v). The heat exchanger vault doors are designed specifically to contain a flood from the VE system. No detailed structural analyses were performed to evaluate the capacity of these doors under realistic loading conditions. However, structural evaluations of other equipment at the plant and analyses at other plants have typically concluded that the likelihood for failure is extremely small under realistic loading conditions, i.e., the structural design safety margin is typically quite large. A nominal value of 1×10^{-6} failure per flooding event was used for f_v.

- Frequency that a Vault Door is Left Open (λ_v). The TF heat exchanger vault doors are normally closed at all times unless work is being performed in a vault. The frequency of maintenance-related flooding events accounts for the fraction of time that a door may be open for maintenance work. Variable λ_v accounts for the combined frequency of other activities that open a door and the likelihood that it might be left open, e.g., special inspections, maintenance or modification planning, etc.

  There is no evidence from plant records or from discussions with plant operations' personnel that any of the TF heat exchanger vault doors has ever been found open during the 12-year period examined for this analysis. However, a conservative upper bound for λ_v was estimated by assuming that any one of the three vault doors may be left open inadvertently approximately once in five years during plant power operation. Therefore:

  $$\lambda_{v\,high} = 1/(3 * 5 * 0.88 * 8{,}760)$$
  $$= 8.65 \times 10^{-6} \text{ error per hour.}$$

  In this calculation, the factor of 3 accounts for the three heat exchanger vault doors; the factor of 5 accounts for the assumed frequency of one error in five years; the factor of 0.88 is the average availability factor for the plant; and the factor of 8,760 converts the annual frequency into an equivalent hourly frequency.

- Annulus Inspection Interval (T). It is assumed for this analysis that a routine inspection of the annulus is performed at least once each shift and that the open door would be discovered during this inspection. Therefore, the average time interval between inspections is eight hours.

These values were used to estimate the following contributions from each condition:

$$\varphi_{SW} f_v = 3.81 \times 10^{-9} \text{ flood per year}$$

$$\lambda_v(T/2)\varphi_{SW} = 1.32 \times 10^{-7} \text{ flood per year}$$

The total frequency of flooding events that are not related to maintenance activities is the sum of these contributions:

$$\varphi_{F,0} = 1.36 \times 1^{-7} \text{ flood per year.}$$

C.3 Frequency of FLOODB

The total initiating event frequency for internal flooding scenario FLOODB is the sum of the two major contributions:

$$\varphi_F = \varphi_{F,M} + \varphi_{F,0}$$
$$= 1.46 \times 10^{-5} + 1.36 \times 10^{-7}$$
$$= 1.47 \times 10^{-5} \text{ flood per year.}$$

The plant model was quantified with the above initiating event frequency and with changes made to the affected event tree top event and system models to reflect the impact of the flood. Specifically, all equipment at the lowest level of the annulus were assumed to be unavailable following the flood.

APPENDIX D
EXAMPLE CONSIDERATION OF A FIRE SCENARIO IN A PRA

An example of a portion of a fire analysis in a recent PRA is summarized in Table D-1. In the scenario summarized in Table D-1, a fire is postulated to occur in the Division 2 Electronics Room affecting all equipment in that room. The analysis of the frequency of all fires in that location, based on the number of electronic cabinets, amount of cable, and the likelihood of transient fire sources had been assessed to have a mean value of 2.11×10^{-5} fire per year. The fire was retained after the screening process that considered only the occurrence frequency. The impacts on the systems considered in the PRA were determined next. These are summarized in the "notes" section of the table in the form of the specific impacts on event tree top events (or split fractions) or system fault trees. The event model is requantified using the fire frequency determined for this scenario along with the system and event level impacts, resulting in a determination of the plant response to fires in this area. The results, in this case, showed that the scenario could be screened from further consideration after this first round of refinement. If that had not been the case, the scenario would have received further attention and refinement. In such a case, the scenario would have been divided into two scenarios: one scenario of relatively low frequency that impacted all the cabinets in the room and a second scenario of relatively high frequency that impacted only the cabinet with the most severe effect on the plant.

Table D-1 Example fire scenario table

BUILDING	E
LOCATIONS	E0456, E0457, E0459
LOCATION NAME	Division 2 Electronics Cabinets Room, Elevation 7.6 meters
LOCATION DESIGNATOR	L2
SCENARIO DESIGNATOR	FIREL2

1. TYPE OF HAZARD SOURCE

2. SCENARIO INITIATION

3. PATH OF PROPAGATION
   A. PATH TYPE — None (localized)
   B. PROPAGATE TO — N/A

4. SCENARIO DESCRIPTION — Fire affects all Division 2 electronics cabinets, including reactor protection.

5. HAZARD MITIGATION FEATURES — Detectors, Halon

6. SCENARIO FREQUENCY — 2.11E-05 per year

7. PRA EQUIPMENT WITHIN THE AREA

Equipment	Top Event	Equipment Impact
Division 2 electronics cabinets	Note 1	Note 1

8. RETAINED AFTER SCREENING ANALYSIS — YES

9. NOTES

This fire scenario affects all cabinets in this room.

1. The impacts from these fires are bounded by disabling all equipment control and actuation signals from Division 2. The following split fraction rules are used to account for the possible impacts from open circuits that may prevent equipment from operating and short circuits that may cause spurious actuation signals.

   - Top Event BB (10 kY nonessential power) is failed.
   - Top Event BY (6 kV essential power) is failed.
   - Top Event S1G2 (Division 2 actuation signal relays) is failed.
   - Top Event REC1 (recovery of offsite power to the 6 kV essential buses) is failed.

Table D-1 Example fire scenario table (cont'd)

- The split fraction rules for Top Events PZRL (pressurizer low level), RCSP (reactor coolant system low pressure), CNTP (containment high pressure), SG IL (steam generator 1 low level), SG2L (steam generator 2 low level), and SG3L (steam generator 3 low level) are modified to account for loss of the Division 2 signals for these fractions.
- The split fraction rules for Top Event TFIS are modified to account for possible loss of the isolation signal for valve TF8OSSOI.
- The split fraction rules for Top Events TFRB and TFSB are modified to account for possible spurious isolation signals for valves TFIOSOS2, TF6OSOOI, and TF605030. Top Events TFRB and TFSB are failed for these fires.
- The split fraction rules for Top Event SUFW are modified to account for possible spurious main feedwater isolation signals for steam generator 2.
- The split fraction rules for Top Event CHF are modified to account for possible spurious isolation signals for valve TA305003. Top Event CHEF is failed for these fires.
- The split fraction rules for Top Event RCPS are modified to account for loss of the Division 2 automatic reactor coolant pump trip signals. Top Event RCPS is failed if reactor coolant pump YD2O is running and nuclear component cooling water flow is lost to the bearing oil coolers.
- The split fraction rules for Top Events LDI, LDO, and CIB are modified to account for loss of the Division 2 isolation signals for the letdown line valves.
- The split fraction rules for Top Event LPC are modified to account for Division 2 isolation signals that prevent RHR cooling from Train TH2O.

NRC FORM 335 (9-2004) NRCMD 3.7 — 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, Rev. 1 BNL-NUREG-52534-R1
2. TITLE AND SUBTITLE Kalinin VVER-1000 Nuclear Power Station Unit 1 PRA Procedures Guides for a Probabilistic Risk Assessment	3. DATE REPORT PUBLISHED MONTH: December — YEAR: 2005 4. FIN OR GRANT NUMBER JCN R2001
5. AUTHOR(S) J. Lehner, et al.	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

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

J. Lane, NRC Project Manager

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 guides, along with training supplied by experts and supplementary material from the literature, were used to advance the PRA carried out for the Kalinin Unit 1 Nuclear Power Station in the Russian Federation. Although written for a specific project, these guides have general applicability. The guides contain procedures for all the technical tasks of a Level 1 (core damage frequency estimation), Level 2 (accident progression/source term analysis), and Level 3 (consequence analysis) PRA. In addition, introductory material is provided to explain the rationale and approach for a PRA. Guidance is also provided related to documentation of PRA results.

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, Level 1, Level 2, Level 3, initiating events, PRA, NPP, internal events, core damage frequency, human reliability analysis, containment analysis, containment performance, radionuclide release, event tree, fault tree, consequence analysis, fire, flood, seismic	13. AVAILABILITY STATEMENT unlimited 14. SECURITY CLASSIFICATION *(This Page)* unclassified *(This Report)* unclassified 15. NUMBER OF PAGES 16. PRICE

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300