NUREG/CR-5637
BNL-NUREG-52260

Generic Risk Insights for Westinghouse and Combustion Engineering Pressurized Water Reactors

Prepared by
R. Travis, J. Taylor, A. Fresco/BNL
J. Chung/NRC

Brookhaven National Laboratory

Prepared for
U.S. Nuclear Regulatory Commission

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 2120 L Street, NW, Lower Level, Washington, DC 20555

2. The Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082

3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Information Resources Management, Distribution Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there 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 the American National Standards Institute, 1430 Broadway, New York, NY 10018.

DISCLAIMER NOTICE

NUREG/CR-5637
BNL-NUREG-52260

Generic Risk Insights for Westinghouse and Combustion Engineering Pressurized Water Reactors

Manuscript Completed: October 1990
Date Published: November 1990

Prepared by
R. Travis, J. Taylor, A. Fresco, Brookhaven National Laboratory
J. Chung, U.S. Nuclear Regulatory Commission

Brookhaven National Laboratory
Upton, NY 11973

Prepared for
Division of Radiation Protection and Emergency Preparedness
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555
NRC FIN A3874

ABSTRACT

A methodology has been developed to extract generic risk-based information from probabilistic risk assessments (PRAs) of Westinghouse and Combustion Engineering (CE) pressurized water reactors (PWRs) and apply the insights gained to Westinghouse and CE plants that have not been subjected to a PRA. The available PRAs (five Westinghouse plants and one CE plant) were examined to identify the most probable, i.e., dominant accident sequences at each plant. The goal was to include all sequences which represented at least 80% of core damage frequency. If the same plant specific dominant accident sequence appeared within this boundary in at least two plant PRAs, the sequence was considered to be a representative sequence. Eleven sequences met this definition. From these sequences, the most important component failures and human errors that contributed to each sequence have been prioritized. Guidance is provided to prioritize the representative sequences and modify selected basic events that have been shown to be sensitive to the plant specific design or operating variations of the contributing PRAs. This risk-based guidance can be used for utility and NRC activities including operator training, maintenance, design review, and inspections.

EXECUTIVE SUMMARY

Background

In this document, a methodology is presented in which generic risk-based information has been extracted from probabilistic risk assessments (PRAs) for pressurized water reactors (PWRs) whose nuclear steam supply systems (NSSS) were designed by Westinghouse or Combustion Engineering (CE). The insights gained have been organized into a matrix format which can be applied to various NRC and utility activities, including inspection, operator training, maintenance and design review, at Westinghouse or CE plants which have not been subjected to a PRA. The relative importance of the insights for each individual plant can be assessed by applying plant-specific modifiers (weighting factors) which vary in degree based on the plant specific design or operating characteristics.

This information can be integrated into various plant programs and activities. Some of the applications include prioritization of maintenance activities, evaluation of plant modifications, operator training, plant configuration controls, and inspections of important contributors to plant risk.

At the time when this methodology was formulated, five PRAs for Westinghouse plants, and one PRA for a CE plant were available in a format suitable for evaluation. It was decided to integrate the results of the six PRAs because the two types of plants, CE and Westinghouse, respond to plant transients in a reasonably similar manner. PRAs for plants with Babcock & Wilcox-designed NSSS were excluded because of the marked differences in plant transient response arising from the relatively small water inventory of the steam generators and from the design characteristics of the integrated control system (ICS).

The NRC has mandated that nuclear power plant licensees develop individual plant evaluations (IPEs) via Generic Letter 88-20. At the present time, it has been reported that 100% of the licensees will respond to the requirements of the generic letter by performing full scope PRAs at least to the level of calculating core damage frequency and containment failure. The methodology presented herein can be used as a check on the completeness of the IPE PRAs.

Methodology Details

The insights gained from this methodology result from the identification of accident sequences which are considered to be representative of the most risk-significant accident sequences of Westinghouse and CE PWRs. These accident sequences are grouped into three categories:

- Loss of coolant accident (LOCA) sequences
- Transient sequences
- Anticipated transient without scram (ATWS) sequences

The six available PRAs were examined to identify the most probable, i.e., dominant, accident sequences at each plant. If a sequence was dominant in two or more plants, it was considered to be a representative accident sequence. Eleven generic accident sequences met this definition.

The core damage frequency distribution among the representative sequences shows marked differences from plant to plant. Such differences are attributable to the design and operational variations. The available PRAs were reviewed to identify the characteristics that determine plant specific vulnerabilities, both with respect to the overall susceptibilities to the particular accident sequences, and to the important basic events. These risk significant features can be used to prioritize both the representative accident sequences and the important basic events.

A summary of the methodology to assess the relative importance of the representative accident sequences and their underlying basic events (component failures and human errors) is provided for Westinghouse or CE plants. For each representative accident sequence, certain of the underlying component failures or human errors are cross-referenced to plant specific modifiers, which are weighting factors used to evaluate the importance of the particular event for the plant in question. The information or insights gained can then be applied to various utility or NRC activities such as operator training, maintenance design review and inspections, with the overall objective of focussing on the most risk-significant areas.

In order to translate the insights of the plant specific evaluation process into a user-friendly format suitable for NRC inspection personnel, a matrix is provided in which the insights from the evaluation of all of the representative accident sequences are reorganized to extract common information as it applies generally to systems. For example, all of the insights applicable to the Auxiliary Feedwater System which happen to arise solely from four representative sequences, are listed under a single heading of "Auxiliary Feedwater System." For each of those insights, which are essentially component failure modes or human errors, the representative sequences in which they occur are listed, as well as the baseline importance estimate for each event. For events which are sensitive to variations in plant design or operating conditions, appropriate plant specific modifiers are cross-referenced. This allows estimation of the plant specific relative importances of components and systems.

The inspection matrix itself consists of columns with the following headings:

(1) Operations
(2) Surveillance
(3) Maintenance
(4) Inservice Inspection/Testing
(5) Calibration
(6) Licensed Operator Training/Emergency Operating Procedures

For each event, the most appropriate areas for inspection focus, e.g., operations or maintenance, are identified.

Risk-Significant, Plant Specific Design Factors

Risk significant, plant specific design factors which can have a significant influence on relative importances of the sequences, systems or components are the following:

- For small break LOCAs, a design which provides automatic switchover from the high pressure injection mode to the recirculation mode is significantly more reliable than a design requiring manual switchover.

- In Westinghouse plants, high pressure recirculation cannot occur directly from the containment sump. The low pressure recirculation system pump(s) must be operational, drawing suction from the containment sump, and discharging to the suction side of the high pressure recirculation pump(s). In CE plants, the high pressure recirculation pumps can draw suction directly from the containment sump.

- For ice condenser containment designs, the smaller free volume results in a faster containment pressurization, as well as earlier spray initiation and depletion of the refueling water storage tank (RWST). The early need for high pressure recirculation eliminates the closed cycle cooling option for the smaller LOCAs. This forces reliance on bleed and feed capability.

- For large break LOCAs, a design which provides automatic switchover from the low pressure injection mode to the recirculation mode is significantly more reliable than a design requiring manual switchover (analogous to the small break LOCA case).

- For LOCAs outside containment, important preventive plant design features are normally closed motor-operated valves in the injection lines to the reactor coolant system, and residual heat removal (RHR) suction line motor-operated isolation valves which are closed and interlocked with RCS pressure for all modes of plant operation except shutdown. (In at least one plant, the interlock is bypassed once the plant is above startup conditions.) An important preventive operating practice is periodic surveillance testing of high to low pressure interfacing check valves upon repressurization of the RCS or after valve movement.

- The importance of the component cooling water (CCW) system is highly dependent upon the assessed integrity of the reactor coolant pump seals for the loss of cooling conditions. In some plants, only the charging pump seals are cooled by CCW while the bearing and motor lubrication systems are cooled by service water (SW). Therefore, the charging pumps would remain operational upon loss of CCW and so RCP seal cooling could be maintained via the normal RCP seal injection flowpaths. Also, in some multi-unit sites, CCW flow can be provided from the other unit upon loss of CCW in one unit.

- The probability of successful decay heat removal is directly dependent upon the diversity and redundancy of the auxiliary feedwater (AFW) system and the feasibility of bleed and feed. Some AFW designs can be severely disabled by the initiating event itself, such as a loss of a 125V DC bus or the loss of the power conversion systems (PCS), such as main feedwater or condensate.

- The degree of redundancy in the emergency AC (EAC) power system is very influential in reducing the probability of Station Blackout (SBO) scenarios. At multi-unit sites, the ability to provide cross-tie power from one unit to the other also has a major impact in reducing SBO probability.

CONTENTS

CONTENTS (cont'd)

TABLES

ACKNOWLEDGEMENTS

The authors wish to thank Charles Willis, Kazimieres M. Campe, and Steven Long of the NRC for their excellent comments and guidance in preparing this document. Our grateful appreciation is also extended to John Boccio and James Higgins of BNL for their expert comments and advice. Also, the services supplied by the BNL Nuclear Research Library under the supervision of Helen Todosow are acknowledged. Finally, to Ann Fort of BNL for the preparation and processing of this document, which led to its successful outcome.

NOMENCLATURE

AFW	Auxiliary Feedwater
B&W	Babcock and Wilcox
BWR	Boiling Water Reactor
CCW	Component Cooling Water
CDF	Core Damage Frequency
CE	Combustion Engineering Company
DC	Direct Current
EAC	Emergency Alternating Current
ECCS	Emergency Core Cooling System
EOP	Emergency Operating Procedure
HPI	High Pressure Injection
HPR	High Pressure Recirculation
ICS	Integrated Control System
ISI	In-Service Inspection
ISLOCA	Interfacing Systems LOCA
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LPI	Low Pressure Injection
LPR	Low Pressure Recirculation
MDP	Motor Driven Pump
MOV	Motor Operated Valve
NRC	U.S. Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply Systems
PCS	Power Conversion System
PORV	Power Operated Relief Valve
PSM	Plant Specific Modifier
PRA	Probabilistic Risk Assessment
PSS	Probabilistic Safety Study
PWR	Pressurized Water Reactor
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RHR	Residual Heat Removal
ROSPA	Risk-Based Operational Safety and Performance Assessment
RPV	Reactor Pressure Vessel
RWST	Refueling Water Storage Tank
SBO	Station Blackout
SDC	Shutdown Cooling
STI	Surveillance Test Interval
SW	Service Water
TDP	Turbine Driven Pump

1. INTRODUCTION

1.1 Objective

The objective of this study was to extract generic risk-based information from available probabilistic risk assessments (PRAs) for Westinghouse and Combustion Engineering (CE) pressurized water reactors (PWRs) for application to plants that have not been subjected to plant specific PRAs. This information is presented in the form of representative (or "typical") accident sequences, and associated basic events, (i.e., component failures, human actions) which can be prioritized by approximating their importance to the frequency of core damage. The accident sequences identified are those representing at least 80% of the total core damage frequency of the plant specific PRAs from which they were derived[1].

1.2 Background

The development of representative accident sequences and the associated PRA design and operating insights was originally proposed for NRC inspection purposes. The intent was to identify typical dominant accident sequences and generate a risk-based ranking of the contributing component failures and human actions. This is intended to provide a rational allocation of inspection resources at Westinghouse or CE plants without PRAs.

This methodology is an outgrowth of a successful plant specific inspection methodology first proposed and implemented by the NRC at Region I. That methodology utilized the plant specific PRA insights to focus on risk important equipment and human actions, and to assess plant response to dominant accident sequences. The principal probabilistic elements included: accident initiators, component failure modes, and human actions which can reduce or exacerbate the accident consequences. These elements are integrated into an inspection matrix format which is used to plan and implement inspections and to evaluate plant performance. The emphasis was placed on relative risk importances of plant equipment and human actions, and the collective contribution of important events to risk of core damage.

1.3 Scope and Limitations

This methodology focuses on core damage for simplicity and ease of application. The scope is generally limited to those systems that are important for the prevention of reactor core damage. The containment and its associated systems are not addressed because not all PRAs calculate the probability of containment failure. All PRAs, by definition, do calculate core damage frequency.

There is a certain degree of design uniformity which can be exploited to provide a generic risk-based overview. However, the plant specific design and operating variations can be a significant influence on both total plant risk and the distribution among the contributing accident sequences.

---

[1] For readers not intimately familiar with PRA terminology, a more detailed explanation of the terms used in this report is provided in Section 5, page 5-1.

This application is limited to the Westinghouse and Combustion Engineering PWR designs. These two types of plants respond reasonably similarly to plant transients. Babcock and Wilcox (B&W) PWRs are not addressed because the plant transient response differs significantly from the aforementioned NSSS designs because of the comparatively small steam generator inventory and the inherent design features of the integrated control system.

Any usable generic application of PRA insights almost by definition, will not address every circumstance likely to be encountered. However, the pertinent methodological details to enable a user to make an informed decision are provided. The accident sequence emphasis allows the key failures and significant plant variations to be presented in a sequence context. This enables understanding of the plant system's design and operational interrelationships that can increase or decrease risk.

1.4 Report Structure and Logic

This risk-based information has many plant applications, as summarized in Section 2. The generation of PRA insights for inspection activities is a major consideration of this program and is the focus of the appendices. Other applications include prioritization of maintenance activities, evaluation of plant modifications, operator training and plant configuration controls. The results of a trial inspection at the Fort Calhoun Station are presented, as well as the major overall insights arising from this effort.

The report then presents the eleven representative accident sequences for Westinghouse or CE PWRs (Section 3) that were developed from the PRAs of six PWRs (see Table 3.1). The representative accident sequences are used as the framework for a discussion of the plant specific design or operating variations that can influence sequence importance. The risk significant plant features are presented for each accident sequence in Section 4 with a qualitative assessment of their impact on sequence importance. The methodology for calculating the contribution of each basic event (component failures and human actions) to the accident sequence frequency is discussed in Section 5.

The overall result is an accident sequence based application of risk insights to Westinghouse and CE PWRs that do not have plant specific PRAs. The methodology is generic. However, risk significant parameters can be incorporated to develop a plant specific ranking of the representative accident sequences and the associated basic events by taking into account plant design and operational variations. These are provided in Table 5.1.

Appendix A presents an inspection matrix which is a composite, ranked listing of the basic events with recommended areas of inspection. Unlike the preceding sections, the matrix is system based because it is more amenable to certain inspection activities. Appendix B provides general guidance on the preparation for a PRA-based inspection and developing the matrix for a particular plant.

2. POTENTIAL APPLICATIONS OF THE METHODOLOGY

Although a plant specific PRA is certainly preferable, this methodology can be used for the inspection of plant activities and operations. The risk significant design and operating features, as well as operating experiences, can be integrated into the representative accident sequences and associated important events to develop plant specific sequences. This, in turn, will provide site-specific risk insights that can be used to prioritize plant activities.

The following summarizes areas of potential applications of the methodology.

2.1 Applications to Plant Operations

2.1.1 Training

This methodology provides plant risk insights and information related to plant strengths and weaknesses in terms of potential core damage accident sequences and associated important contributors or accident initiators. They may consist of failures of plant components or human actions or combination of such events. These insights can be factored into the training program of plant personnel including licensed control room operators.

Simulation of dominant accident sequences on a simulator can provide the plant operators valuable training to cope with the most probable accidents. Such exercises in parallel with the Emergency Operating Procedures (EOPs) will provide them insights and training of the plant vulnerability, beyond single failure criteria, so as to mitigate and/or to recover from the event situations. The objective is to familiarize them with the potential plant vulnerability, and thus to minimize the potential human errors should such events occur.

2.1.2 Plant Configuration Control

It is common practice in a nuclear power plant to maintain a critical component list that contains the plant safety-related components and energy production-related equipment, as well as those added by plant management. Such critical components may vary from one plant to another, even among the plants with similar design. The plant critical components can be prioritized on the basis of the relative risk importances for maintenance and surveillance schedules. This will minimize unavailability of the critical components, and thus reduce system unavailability. Application of the risk insights for the plant configuration control can reduce the plant risk by minimizing potential accident initiators and may improve plant availability.

Critical safety systems may be selected on the basis of risk insights for preventing plant damage resulting from a severe accident or extended plant outages. The unavailable hours of the selected safety systems and associated components can be trended to form a basis for the plant performance indicators. Appropriate application of the reliability concept in conjunction with the risk insights can reduce undue extended outages of critical components for maintenance or surveillance, and can provide a basis for good predictive and preventive maintenance program.

2.1.3 Design Review and Technical Specifications

Because of the generic nature of the methodology, the insights developed from this methodology may not be adequate to use for assessment of Surveillance Test Interval (STI) nor to evaluate maintenance outages of the critical components or systems. However, the methodology can be used for a comprehensive understanding and interpretation of an intent of Technical Specifications, particularly should the wordings and conditions in the Technical Specifications need further clarification or be ambiguous.

Another application is a review process of plant modifications and back-fit issues. A relative change in risk may be evaluated qualitatively due to changes in plant conditions.

2.1.4 Plant Inspections

The objective of a plant inspection is to evaluate the plant programs and their implementation to verify that the plant is operating and maintained at an acceptable level of risk. However, inspection resources and sample sizes are usually limiting factors for inspection activities.

The inspection items and activities can be prescribed on the basis of the risk insights - prioritization of important plant events and probable failure modes of the important events. The prioritization of inspection items and development of an inspection plan are discussed in Appendices A and B.

2.2 Trial Application of the Methodology at the Fort Calhoun Station

This methodology was used to perform a Risk-Based Operational Safety and Performance Assessment (ROSPA) at the Fort Calhoun Station in October, 1989 (Refs. 1 and 2). The generic information was revised to reflect the Fort Calhoun design and operating practices, gleaned from a technical specification and FSAR review. The representative accident sequences were prioritized. Generally, unless there was some information to the contrary, the sequences were considered highly important. One sequence was eliminated because the plant does not utilize low pressure recirculation. Other sequences were downgraded in importance. These actions were taken because of the relatively greater integrity of the reactor coolant pump seals upon loss of cooling and a high to low pressure interface design that features normally closed motor operated valves. All sequences with AFW input were considered highly important because the plant design consists of only two AFW pumps. As part of this inspection, two of the "high importance" sequences were chosen for control room simulations using an off duty crew. In addition to the sequence level input, the generic inspection matrix was modified to reflect the Fort Calhoun design. Inappropriate systems components or human actions (such as the low pressure recirculation mode or manual switchover to high pressure recirculation) were deleted. Additional plant specific system interactions, design features, or operator actions that could prove useful to prevent or mitigate the representative accident sequences were added to the scope of the inspection including:

- temperature indication to monitor the AFW pump discharge piping for back leakage from main feedwater
- the use of the Raw Water Cooling System as a manually aligned backup to CCW for ECCS pump cooling

- ECCS non-dependency on pump room cooling
- the plant specific bleed and feed capability

The inspection cycle included two weeks of on site inspection. There were two distinct efforts. The majority of the team was associated with the system/component based inspection effort, using an inspection matrix (see Appendix A) to prioritize their inspection efforts. As with other team inspections, the inspectors used the NRC inspection manual (Ref. 2), past plant/industry history and their own experience to develop their own avenues of inquiry, for the selected items.

The second effort was more operations oriented and consisted of a control room simulation of two representative accident sequences that were assessed to be of high importance. The team included a Region IV license examiner who prepared plant specific accident scenarios. The scenarios simulated the two sequences, including plant specific timing considerations and operator cues to provide plant information that would normally be available in the control room. This phase of the inspection provided valuable insights on operator training and procedural adequacy that are not obvious in a system oriented inspection. By concentrating on the important component failures or unavailabilities, and the operator actions in response to those failures or unavailabilities, the plant operational readiness and safety performance was evaluated.

The application of the methodology was considered successful. The other participants in the inspection provided valuable feedback, and their overall assessment, to the authors of the methodology such as:

- The PRA-based prioritizaton of the plant's systems and components enabled the inspection effort to focus on risk significant items.
- The control room simulation of two representative accident sequences uncovered unexpected procedural weaknesses.

The PWR inspection matrix, which provides a prioritization of the important PRA events, is presented in Appendix A. The development of a risk-based inspection plan is discussed in Appendix B.

2.3 Major Risk Significant Insights

The results of this study indicate that the insights which have the greatest risk significance are the following:

- A high pressure injection (HPI) design that provides automatic realignment to the recirculation mode, as compared to one requiring manual changeover, results in greater resistance to a small break LOCA with loss of high pressure recirculation.
- The Westinghouse design uses low pressure ECCS as a support system for high pressure recirculation (HPR). This dependency is not present in the CE design.
- For ice condenser containment designs, the smaller free volume results in faster containment pressurization, earlier spray initiation and a quicker RWST depletion. The early need for HPR eliminates the closed cycle cooling option for smaller LOCA initiators.

- A low pressure ECCS design that provides automatic realignment to the recirculation mode (LPR) results in greater resistance to a large LOCA with failure of LPR.

- The plant specific contribution to the LOCA outside containment sequence is influenced by design (normally closed injection line MOVs, full time shutdown cooling pressure interlock) and operating practices such as a requirement for testing the interface check valves at RCS repressurizations or after valve movement.

- The importance of the component cooling water (CCW) system is highly dependent upon the assessed integrity of the reactor coolant pump seals for loss of cooling conditions. In some plants, only the charging pump seals are cooled by CCW while the bearing and motor lubrication systems are cooled by service water (SW). Therefore, the charging pumps would remain operational upon loss of CCW and so RCP seal cooling could be maintained via the normal RCP seal injection flowpaths. Also, in some multi-unit sites, CCW flow can be provided from the other unit upon loss of CCW in one unit.

- The probability of successful decay heat removal is directly dependent upon the diversity and redundancy of the auxiliary feedwater (AFW) system and the feasibility of bleed and feed. Some AFW designs can be severely disabled by the initiating event itself, i.e., the loss of 125V DC bus.

- The degree of redundancy in the emergency AC (EAC) power system is very influential in reducing the probability of Station Blackout (SBO) scenarios. At multi-unit sites, the ability to provide cross-tie power from one unit to the other also has a major impact in reducing SBO probability.

When these features are incorporated into the methodology, a plant specific ranking of representative accident sequences, component failures, and human actions can be developed. This information can be integrated into ongoing plant activities, including operator training, maintenance, design review and inspections. This helps to emphasize the risk significant areas accordingly.

3. DEVELOPMENT OF REPRESENTATIVE ACCIDENT SEQUENCES FOR WESTINGHOUSE AND CE PWRs WITHOUT PLANT RISK ASSESSMENTS

This section presents the first phase of the methodology. Risk insights from PRAs of Westinghouse and CE PWRs that were available were extracted for application to other PWRs not already subjected to a PRA. As explained in Section 1, risk assessments were used as a data base to develop eleven PWR representative accident sequences. These sequences form the basis of a generic PRA application that will examine plant specific influences on sequences importance and basic event prioritization, as described later in this report.

3.1 Establishment of the PRA Data Base

The initial objective was to focus on Combustion Engineering Plants. However, the extent of the risk assessment material that was available for these plants (specifically, accident sequence cutsets) was very limited. Therefore, Westinghouse PWRs were included in the PRA data base as the two designs are very similar. Since dominant accident sequence descriptions were readily available for six plants, their respective PRAs form the data base, as listed in Table 3.1, used to develop the representative accident sequences for this program.

3.2 The Representative PWR Accident Sequences

Each risk assessment was reviewed to develop a set of plant specific dominant accident sequences. As shown in Table 3.2, at least 10 sequences with the highest contribution to core damage were specified in an attempt to capture 80% (minimum) of the plant core damage frequency. If the accident sequence makeup precluded the attainment of the 80% goal with a reasonable number of sequences, the plant specific dominant accident set was truncated when the last sequence contributed approximately 1E-6/reactor year to the plant core damage frequency. The six sets of plant specific dominant accident sequences were compared. **If a sequence was present in two or more plant specific listings, it was designated as a representative accident sequence.** This criterion resulted in the exclusion of accident sequences associated with the loss of service water, steam generator tube rupture and the loss of instrument air initiators. The six sets of plant specific dominant accident sequences did not contain any of these sequences. Two sequences (LOCA outside containment and loss of PCS) barely satisfied the criterion and some consideration was given to eliminating them from the list of representative accident sequences. They were retained as discussed below.

For simplicity and ease of application, this program utilizes core damage frequency as the measure of risk. In general, accident sequences that are dominant with respect to a core damage frequency risk measure also appear if a health effects measure is employed, with one major exception. From a core damage perspective the LOCA outside containment is not a significant contributor. However, when a health effects measure is employed, the bypassing of the containment plays a key role with respect to offsite consequences. Hence, this sequence becomes significantly more important. In an attempt to envelope both risk measures with a single set of representative accident sequences, the LOCA outside containment sequence has been retained. Table 3.3 presents the representative PWR accident sequences.

Table 3.4 shows the fraction of core damage frequency that is accounted for by the representative sequences. The fraction in Table 3.4 is typically less than that of the plant specific dominant accident sequences, because not all can be correlated with a representative accident sequence. However, these representative sequences generally capture a significant portion of the plant core damage frequency. The results tend to be understated as the methodology also addresses other non-dominant sequences. This is noted in Table 3.4 by the "+" which indicates those representative sequences that capture a small fraction of the core damage frequency attributable to plant specific non-dominant sequences which are similar to the dominant sequences.

For example, the Surry PRA (Ref. 4) analyzes the top 20 sequences representing 99% of the total core damage frequency (CDF). As previously stated in Table 3.2, this methodology utilized the top eleven sequences (81% of the Surry CDF) to develop the representative sequences. Since three of the eleven Surry dominant sequences are not addressed by the representative sequences, Table 3.4 shows a lower fraction of core damage frequency (62%) than is captured by the representative sequences.

However, the representative sequences also address similar, non-dominant sequences. Representative sequence number 2 envelopes the Surry number 12 and 18 accident sequences. Non-dominant sequences also provide significant contributions to representative sequences 1, 3, and 11. Hence, the "+" sign is inserted for those sequences in Table 3.4. The fraction of CDF that is captured by the representative sequences, based on the top twenty Surry accident sequences, is 78%.

The contribution of the non-dominant accident sequences is especially important for Millstone. The Millstone 3 Probabilistic Safety Study (PSS) (Ref. 5) is characterized by a large number of sequences. No single sequence makes a major contribution to the core damage probability; the leading sequence contributes only 8.5% to the total. Other similar sequences contribute to the "12+" shown in Table 3.4 for Representative Sequence No. 1. The top ten represent only 43% of the total. This can be attributed, in part, to the large number of specific initiators that were used. For example, instead of a generalized small LOCA event tree, the Millstone PSS also includes a separate event tree with in-core instrument tube rupture as the initiating event. Representative sequence 1, Small LOCA with Failure of High Pressure Recirculation, addresses both of these Millstone sequences. The NUREG/CR-4142 (Ref. 6) event trees were reviewed to estimate the total core damage fraction that could be accounted for by the methodology. All sequences with a contribution of 1E-7 or greater were reviewed. Approximately 63% of core damage frequency would be addressed by the methodology.

Table 3.4 also provides the distribution of the six plant specific core damage frequencies among the representative accident sequences. The distribution is consistent with the risk assessments that were used as the data base since it reflects the range of core damage contributors. This resulted in the specification of a larger number of representative sequences to ensure that the methodology is applicable to a typical Westinghouse or CE plant.

Section 4 expands the representative accident sequence descriptions and provides an assessment of features that can influence plant specific sequence importance.

Table 3.1 PRA Data Base Used to Develop the Representative Accident Sequence List

Plant	NSSS Vendor [1]	PRA Documents
1. Calvert Cliffs Unit 1*	CE	Interim Reliability Evaluation Program: Analysis of the Calvert Cliffs Unit 1 Nuclear Power Plant, NUREG/CR-3511, March 1984.
2. Sequoyah, Unit 1*	W	Analysis of Core Damage Frequency from Internal Events: Sequoyah, Unit, NUREG/CR-4550, Vol. 5, February 1987.
3. Surry, Unit 1*	W	Analysis of Core Damage Frequency from Internal Events: Surry, Unit 1, NUREG/CR-4550, Vol. 3, November 1986.
4. Zion, Unit 1*	W	System Analysis and Risk Assessment System, (SARA) User's Manual (Draft) Version 3.0, NUREG/CR-5022, September 1987. Analysis of Core Damage Frequency from Internal Events: Zion Unit 1, NUREG/CR-4550, Vol. 7, October 1986.
5. Indian Point, Unit 3	W	Review and Evaluation of the Indian Point Probabilistic Safety Study, NUREG/CR-2934, December 1982.
6. Millstone, Unit 3	W	A Review and Evaluation of the Millstone 3 PSS, NUREG/CR-4142, April 1986. Probabilistic Risk Assessment (PRA) Insights, NUREG/CR-4550, January 1986.

* Also used to formulate system and basic event importances.

[1] CE = Combustion Engineering
W = Westinghouse

Table 3.2 Plant Specific Dominant Accident Sequence Criteria

Plant	Number of Plant Specific Dominant Accident Sequences Comprising at Least 80% of Core Damage Frequency	Percent of Total Core Damage Represented by the Dominant Sequences	Number of Plant Specific Dominant Accident Sequences Addressed by the Methodology[2]	Percent of Core Damage Frequency Addressed by the Methodology
Sequoyah, Unit 1	10	94	10	94
Surry, Unit 1	11	81	8	62
Calvert Cliffs, Unit 1	11	83	8	80
Zion, Unit 1	10	>99	7	>99
Indian Point, Unit 3	10	>99	10	>99
Millstone, Unit 3	10	43[1]	7	32[3]

1 If the 80% goal could not be satisfied with a manageable number of sequences, the plant specific dominant accident set was truncated when the last sequence contributed approximately 1E-6/reactor year.

2 If a sequence appears in two or more plant specific PRA dominant accident sequence listings, it is designated as a representative sequence.

3 The Millstone Probabilistic Safety Study has a large number of similar accident sequences. No single sequence makes a major contribution to the core damage frequency; the leading sequence comprises only 8.5% of the total. Other similar sequences comprise the 12+% of Representative Sequence No. 1 shown in Table 3.4.

Table 3.3 Representative PWR Accident Sequences

Loss of Coolant Accident Sequences

1. Small or medium LOCA with failure of high pressure injection or recirculation.

2. Medium or large LOCA with failure of low pressure recirculation.

3. Medium or large LOCA with failure of low pressure injection.

4. LOCA outside containment.*

Transient Sequences

5. Loss of all CCW with a subsequent RCP seal LOCA.

6. Loss of 125V dc bus with failure of the Auxiliary Feedwater System (AFW).

7. Loss of offsite power (LOOP) with failure of AFW and bleed and feed.

8. Station blackout with loss of the AFW system.

9. Station blackout with a subsequent RCP seal LOCA.

10. Loss of PCS (or a general transient with loss of PCS) followed by loss of AFW.**

Anticipated Transient Without Scram (ATWS) Sequences

11. Transient with failure to automatically and manually scram followed by failure of timely emergency boration.

---

* Specified because of serious consequences.

** Specified based on a review of the studies that established precursors to potential severe core damage accidents (NUREG/CR-2497, 3591, 4674).

Table 3.4 Plant Specific Core Damage Distribution

Represent. Sequence # (from Table 3.3)	Percent of Core Damage Frequency (CDF)					
	Sequoyah Unit 1	Surry Unit 1	Calvert Cliffs Unit 1	Zion Unit 1	Indian Pt. Unit 3	Millstone Unit 3
1	56	14+	19+	11	8	12+
2	1	+		7	28	3+
3	<1	+		1	3	+
4	+	4		+	+	4
5	31**			79	50	
6	2		16	+		5+
7		4	4+			4+
8	1	19	3	2		4+
9	3	26			1	+
10			11+		1	+
11	+	4+	27+		9	+
Dominant Accident Total*	94	62	80	>99	>99	32

* The core damage frequency accounted for by the representative accident sequences is a significant portion of the plant total. The dominant accident total understates the methodology effectiveness. As indicated above by a "+", the representative sequences also capture a portion of the CDF attributable to similar non-dominant sequences. This is especially significant for Millstone 3, which has a large number of similar accident sequences. Based on a review of the NUREG/CR-4142 event trees, approximately 63% of the total CDF is addressed by the methodology, not just the apparent 32%.

** When this methodology was originally prepared in 1988, the Sequoyah PRA, NUREG/CR-4550, Vol. 5, indicated that loss of the CCW system led to the total failure of the chemical and Volume Control System charging pumps, which provide injection flow and cooling to the reactor coolant pump seals. Since CCW also cools the RCP thermal barrier heat exchangers, it was assumed that loss of CCW would lead directly to a RCP seal LOCA. Subsequently, it was determined that only the charging pump seals are cooled by CCW. The bearings are cooled by service water so the pumps could remain functional and a RCP seal LOCA would not necessarily occur. The contribution of this sequence is consequently reduced significantly from the 31% shown.

4. PLANT SPECIFIC DESIGN AND OPERATING INSIGHTS

As previously discussed, Table 3.4 provides the core damage frequency (CDF) distribution of the surrogate plants among the representative accident sequences. For any given sequence there is a significant variation in CDF contribution from plant to plant. Again, the objective is to capture at least 80% of the plant's core damage frequency by considering the eleven representative sequences.

The major plant specific design and operating variations are discussed within the context of each representative accident sequence. In Table 4.1, the representative accident sequences are qualitatively prioritized by the assessed availability of key systems. The Indian Point 3 and Millstone 3 PRAs did not provide detailed dominant accident sequence failure modes (cutsets) so no specific system assessments could be made for those plants and they do not appear in Table 4.1.

4.1 Representative Accident Sequence 1: Small or Medium LOCA with Failure of High Pressure Injection or Recirculation

Sequence Description

Representative Accident Sequence 1 is initiated by a small or medium LOCA which does not depressurize the Reactor Coolant System (RCS) below the shutoff head of the low pressure ECCS. RPS successfully scrams the reactor. The sequence postulates high pressure ECCS failure to provide adequate RCS makeup either in the injection or the recirculation phases, resulting in core damage. The PRA initiator is a small or intermediate primary system pressure boundary failure less than six inches in diameter. Commercial nuclear power plant pressure boundary failures have been limited to small LOCAs with equivalent rupture diameters less than two inches and consist of stuck open PORVs and, to a lesser extent, RCP seal failures.

The failure to provide adequate core makeup in the high pressure injection (HPI) phase is a significant contributor to this sequence. This contributor is dominated by valve failures in the HPI common discharge or suction lines.

Failures in the high pressure recirculation (HPR) mode dominate this sequence. These can occur in the HPR system or in any of the support systems required for long term LOCA mitigation. The HPR failures are dominated by operator failure to correctly realign the system from the injection mode (for manual systems) or valve failures in the common discharge or suction lines on the mini flow line for those configurations with automatic realignment to the HPR mode. The Westinghouse HPR configuration takes suction from the low pressure recirculation (LPR) pump discharge. LPR malfunctions that disable HPR are the second major contributor to HPR failures. The primary faults are LPR suction (containment sump) valve and pump malfunctions.

HPR room cooling failures are the last major contributor. These are attributable to electrical component failures that disable room cooler fans or service water valve failures that disable the coolers themselves. Refueling water storage tank (RWST) common mode level sensor miscalibration and service water/component cooling water malfunctions that disable the HPR pump coolers are less important failures.

Plant Specific Design and Operating Insights

The plant specific core damage frequency contributions to representative accident Sequence 1 range from 56% (Sequoyah) to 8% (Indian Point 3). Although the other plant contributions to this sequence are not insignificant, Sequoyah is relatively vulnerable to the small/medium LOCA initiator. As previously discussed, the critical recovery action is successful high pressure ECCS, both HPI and HPR.

The four reference plants (Sequoyah, Surry, Calvert Cliffs and Zion) with accident sequence information were reviewed to assess the contribution of plant specific design and operating variations to this sequence.

The major design features that can influence risk are:

- Manual (Sequoyah) or automatic (Surry, Calvert Cliffs, Zion) realignment to high pressure recirculation. The need for early operator action to ensure continued HP ECCS is the key contributor to Sequoyah's large contribution to Sequence 1. Thus timing is critical for ice condenser containments, as discussed below.

- Limited, automatic HPI injection paths in conjunction with normally closed MOVs (Surry) as opposed to normally open MOVs and/or multiple RCS injection pathways.

- A common RWST suction line for HPI (Surry) has higher assessed unavailability due to suction valve failures. Plants with multiple suction lines (i.e., separate charging and safety injection suction configurations) reduce this failure contribution.

- The use of the low pressure ECCS in the recirculation mode as a support system for the Westinghouse high pressure recirculation design. Unlike Combustion Engineering designs (Calvert Cliffs), continued LPR operability is essential for small LOCA mitigation.

- Among the Westinghouse units, low pressure recirculation is even more important for plants with ice condenser containments. The free volume is smaller than in large dry containments causing faster pressurization which, in conjunction with a lower spray setpoint, activates the sprays earlier. The relatively lower containment design pressure requires earlier actuation of the spray system. Also, the spray system flow rate is higher than that in a large, dry containment. This in turn, results in an earlier need for recirculation. It has been estimated that a small LOCA at Sequoyah could require a switchover to the recirculation mode in about 80 minutes from the beginning of the accident or about 20 minutes after containment spray actuation. For the same size break, a large dry containment would not require recirculation switchover for several hours, giving the operator time to lower the RCS temperature, depressurize and transfer to closed cycle shutdown cooling. The accelerated timing for the smaller ice condenser containment design does not allow this.

- Normally closed LP ECCS miniflow valves can contribute to LPR failure due to pump overheating during the injection phase. A design that features normally open miniflow valves with out of position annunciation in the control room eliminates this concern.

Qualitative Estimate of Sequence Importance

The foregoing assessment of the plant specific ECCS design variations, in conjunction with the CDF contributions of Table 3.4, indicates that representative accident sequence 1 is generally highly important. At Sequoyah this sequence is of "very high" importance, primarily because of the lower assessed success rate of the manual realignment to high pressure recirculation. Table 4.1 presents the importance estimates for all eleven representative accident sequences, resulting from the assessed availability of key functions and systems.

4.2 Representative Accident Sequence 2: Medium or Large LOCA with Failure of Low Pressure Recirculation

Sequence Description

Representative accident sequence 2 is initiated by a medium or a large LOCA which rapidly depressurizes the reactor coolant system. A scram occurs, followed by successful operation of the Low Pressure Injection (LPI) system. When the refueling water storage tank (RWST) is depleted, an automatic or manual realignment of the LP pump suction to the containment sump must occur.

This sequence postulates low pressure recirculation (LPR) system failure. Due to the loss of primary system injection, core damage occurs. The PRA initiator is a medium (effective break diameter of 2 to 6 inches) or a large (effective break diameter of 6 to 29 inches) primary system pressure boundary failure. No actual industry failures of this magnitude have occurred. Commercial nuclear power plant pressure boundary failures have been limited to small LOCAs with equivalent rupture diameters less than two inches. The major contributor to core damage for this sequence is the failure of the low pressure ECCS in the recirculation mode. LPR system failure is evenly divided between human errors and hardware failures. The dominant human error contributor is the failure to initiate LPR by manual realignment of the pump suction from the RWST to the containment sump. This failure dominates those plants with non-automatic pump suction realignment. A second operator error is the failure to manually switch the LPR pump discharge from cold leg to hot leg injection.

Hardware failures are the dominant contributors to LPR system failure for those plants with an automatic pump suction changeover feature. Important valve malfunctions include failures of LPR containment sump valves to open or RWST suction valves to close, including common cause failures. The failure of the low pressure pumps to continue to run (including common cause) is the remaining LPR hardware failure. The common cause miscalibration of the RWST level sensors is the only major failure not directly associated with the low pressure (LP) ECCS.

Plant Specific Design and Operating Insights

The CDF contributions associated with representative sequence 2 are generally small, reflecting the lower likelihood of a large LOCA. Although modest, the plant specific contributions of Table 3.4 do vary, from 7% for Zion to approximately 1% for Sequoyah, to very small for Surry. The sequence is not applicable to Calvert Cliffs since the CE design uses the high pressure ECCS for the mitigation of all LOCAs. The LP ECCS is generally locked out by the same low RWST signal that automatically realigns the HPI to the recirculation mode.

The major design element that influences the sequence importance is the automatic low pressure ECCS alignment to the containment sump. The Zion system requires manual alignment of recirculation; Sequoyah has partially automatic switchover. In general, manual non-routine actions under high stress conditions have a lower assessed success rate than the equivalent automatic function. This is the primary difference between the Zion and Sequoyah CDF contributions.

Qualitative Estimate of Sequence Importance

As stated above, the assessed availability of the low pressure recirculation (LPR) mode determines the importance of this sequence. Representative accident sequence 2, is generally of medium importance in Table 4.1, reflecting the "average" success estimate for the fully automatic LPR design. Zion, however, requires operator action to align LPR, resulting in a somewhat higher sequence importance estimate. Since the high pressure ECCS is utilized for all LOCA sizes, the sequence is not applicable to Calvert Cliffs.

4.3 Representative Accident Sequence 3: Medium or Large LOCA with Failure of Low Pressure Injection

Sequence Description

This sequence is initiated by a medium or a large LOCA which depressurizes the reactor coolant system. A scram occurs, followed by a failure to provide core makeup via the low pressure injection system or the accumulators. Core damage ensues.

The initiator is a medium or a large primary system pressure boundary failure in the reactor coolant system 2 inches and larger in diameter. Although failures of this magnitude have been commonly postulated in risk assessments, no medium or large LOCAs have occurred in the domestic commercial nuclear power industry.

The major contributor to core damage for this sequence is the failure to provide short term core injection i.e., due to failures of accumulator or low pressure injection. The success criteria to prevent core damage is usually that one out of two RHR pumps and three out of four accumulators deliver flow to the RCS. For a large LOCA the flow from the accumulator on the ruptured loop would be ineffective. A second accumulator failure, resulting in core damage, is attributed to discharge line failures, primarily check valve failures to open or MOV plugging. The Low Pressure Injection (LPI) system failure is dominated by pump failure to start or run, including common cause. Human error contributors are the failure to restore the system to operable status after testing and the failure to stop the pumps if the mini flow valve fails to open.

Plant Specific Design and Operating Insights

The plant specific core damage frequency contributions associated with sequence 3 are small. As shown in Table 3.4, only one plant design contributes more than 1% of its total CDF to this sequence, (i.e., Indian Point 3 at 3%). The assessed low pressure injection unavailability, although comparatively low, can be influenced by the following plant design features:

- Redundant accumulator level and pressure instrumentation on the accumulators helps ensure that injection failures are not due to loss of inventory or nitrogen pressure.

- Accumulator and low pressure injection MOV misposition alarms and/or automatic opening on a safety injection signal reduce the failure contribution due to system misalignment. In lieu of these design attributes, system valve positioning could be periodically verified by an operator.

- The normal position of the LP ECCS miniflow valves can be important for RCS failures at the low end of the medium LOCA spectrum. These failures will depressurize the RCS more slowly and LPI pump deadheading is a concern. Normally closed miniflow valves (Sequoyah) must open to preclude pump damage; normally open valves perform this function passively.

Qualitative Estimate of Sequence Importance

Although the surrogate plants exhibit several low pressure ECCS design variations, these features do not appear to significantly affect risk. Based on the plant specific core damage frequency (CDF) contributions, sequence 3 is of medium importance for all plants.

4.4 Representative Accident Sequence 4: LOCA Outside Containment (or Interfacing Systems LOCA: ISLOCA)

Sequence Description

The ISLOCA is initiated by either a failure of any one of the pairs of series high to low pressure interface check valves or MOVs that isolate the high pressure Reactor Coolant System (RCS) from the Low Pressure Injection (LPI) system, or by the inadvertent opening of the shutdown cooling suction line. The resultant flow into the low pressure system is assumed to rupture the piping or components outside the containment boundary. Although core inventory makeup by the high pressure systems is initially available, the inability to switch to the recirculation mode eventually leads to core damage.

The NRC is currently evaluating certain previous and current event reports at both domestic and foreign plants to determine if they should be categorized as ISLOCA precursors. PWR check valve and MOV test procedures should be examined carefully to ensure the potential for a test induced LOCA outside containment is minimized. [A similar LOCA outside containment scenario can occur in boiling water reactors (BWRs). Several BWRs have experienced pressurizations of the low pressure piping, primarily due to testing errors.]

The discharge of the LPI system generally consists of one or two low pressure injection lines with a normally open MOV. Downstream of this MOV (toward the RCS) the piping is rated for primary loop conditions. The discharge line(s) divides to connect to each RCS cold leg. Each of these individual lines has two check valves in series. Small leakages through these valves can be accommodated without system overpressure. The failure modes of interest produce sudden, large back leakages through a pair of these interface check valves. The LPI failure is postulated to occur in three ways:

- The dominant LPI initiator mode is the rupture of one check valve with the previously undetected opening of the second valve. If one valve is holding pressure, the other valve can drift open and fail in the open position.

- The second initiator mode is the failure of one check valve to close upon repressurization, followed by a rupture of the second valve.

- The third initiator type is the random rupture of the valve internals for both check valves. The gross failure of one valve could go undetected until the rupture of the second valve occurs.

A second initiator is the overpressurization and failure of the shutdown cooling suction line. The two, suction line MOVs, which are normally closed, are postulated to rupture or the downstream check valve oscillates open with a subsequent rupture of the upstream valve.

Plant Specific Design and Operating Insights

With the possible exception of Calvert Cliffs, all of the plant PRAs indicate some risk associated with the containment bypass LOCA sequence. The primary determinant of each plant specific contribution is the estimated initiator frequency which, in turn, is influenced by the high to low pressure configuration and plant procedures. Specific design and operating considerations are:

LPI Interface

- The high to low pressure interface design of Calvert Cliffs features several check valves in series with a normally closed MOV. The check valves are periodically leak tested and the MOV is tested only when the RCS is depressurized. Other CE plants may have similar features.

- The placement of the accumulator discharge relative to the high/low pressure interface can influence the check valve failure order. For example, Sequoyah's accumulators connect between the two check valves. If the upstream check valve (furthest from the RCS) fails first, the accumulator will discharge into the LPI system and alert the operator. If the interface check valves can fail in any order (i.e., Surry) this initiator is more likely.

- Failure of a check valve to close upon RCS repressurization is not a concern if plant operating procedures require the testing of the interface check valves during every RCS repressurization or if the valves change position.

Shutdown Cooling Interface

- The shutdown cooling configuration generally features two normally closed MOVs in series with a relief valve in between. The intervening relief valve makes it necessary that the downstream MOV (furthest from the RCS) fail first. Otherwise, the relief valve discharge would alert the operator and plant shutdown would commence.

- The shutdown cooling line initiator can be neglected if the MOVs have a high pressure interlock to prevent downstream piping overpressurization and the MOVs are key locked with administratively controlled keys (Calvert Cliffs).

Recovery

A potential recovery action has been included to account for operator action to isolate the ISLOCA by manual closure of the LPI discharge MOV. The successful mitigation of this event is plant specific and is dependent on:

- The existence of two isolable LPI discharge headers to enable the use of the other LPI loop, or the ability to use another system for RCS makeup.
- LPI pump separation to minimize the environmental impact of RCS blowdown on the second train.
- The capability of the LPI discharge MOV to isolate the ISLOCA. The value may not be designed to close against such a high differential pressure.

Qualitative Estimate of Sequence Importance

Representative Sequence 4 is generally considered to be a low importance sequence from a core damage perspective. However, from a health effects perspective this sequence is significantly more important because the containment is bypassed. The limited response measures to a LOCA outside containment make the LPI and SDC interface design the determinant of sequence importance. As summarized in Table 4.1, the SDC interface integrity is generally considered to be average, with the exception of Zion where an interface valve interlock is bypassed during power operation. The low pressure injection interface integrity is considered to be average if the check valves fail in a particular order due to the placement of the accumulator discharge. Calvert Cliffs has been assigned a high estimated integrity since the normally closed LPI MOVs are tested only when the RCS is depressurized.

4.5 Representative Accident Sequence 5: Loss of all CCW Initiator

Sequence Description

Representative Sequence 5 is initiated by a complete loss of the Component Cooling Water (CCW) system which results in a reactor coolant pump (RCP) seal LOCA and also disables the high and low pressure ECCS. This happens because the CCWS cools the RCP seals thermal barrier heat exchanger and also cools both the CVCS charging pump bearings and seals. If CCWS is lost, the charging pumps would ultimately fail, thereby preventing the normal RCP seal injection flow which also cools the RCP seals. The joint failure of the RCP seal injection flow and the charging pumps, which also provide high pressure makeup flow in the HPI mode, (i.e., the high pressure ECCS) fails the RCP seals. The inability to provide high pressure makeup results in core damage. One major contribution to the loss of CCW initiator is a pipe rupture that drains the system inventory before the break can be located and isolated. The second contribution is the common cause failure of all operating CCW pumps, compounded by a failure of the standby pump(s) to start and run. The RCP seal LOCA and subsequent core damage is postulated to occur before CCW recovery actions can be completed.

Table 4.1 Representative Sequence Priorization Summary[1]

Repres. Sequen.	Ref. Plant	Sequen. Import.	Qualitative Success Estimate for Critical Functions and Systems													
			HPI/R	LPI/R	Accum.	LPI Interface Integ.	SDC Interface Integ.	RCP Seal Integrity	RCP Seal Cooling	AFW	Bleed and Feed	Emerg. AC Power	DC Power	RPS	Manual Scram	Emerg. Borat.
1	Sequoy. Surry Calv. Cl. Zion	higher high high high	lower lower average lower	lower average N/A average												
2	Sequoy. Surry Calv. Cl. Zion	medium medium N/A high		average average N/A lower												
3	Sequoy. Surry Calv. Cl. Zion	medium medium medium medium		average average average average	average average average average											
4	Sequoy. Surry Calv. Cl. Zion	low medium lower low				average lower higher average	average average average lower									
5	Sequoy. Surry Calv. Cl. Zion	high[2] low low high						average average higher average	average higher average average							
6	Sequoy. Surry Calv. Cl. Zion	medium low high low								average average lower average	N/A average N/A higher					
7	Sequoy. Surry Calv. Cl. Zion	low low medium low								average average lower average	average average N/A higher					

[1] See the text for a discussion of critical function and system availability.

[2] The latest revision of NUREG/CR-4550, Vol. 5 indicates that this sequence is of significantly lower importance at Sequoyah because the HPI pumps (i.e., CVCS charging pumps) do not fail to operate upon loss of CCW. See second footnote to Table 3.4.

Table 4.1 (Cont'd)

Repres. Sequen.	Ref. Plant	Sequen. Import.	Qualitative Success Estimate for Critical Functions and Systems														
			HPI/R	LPI/R	Accum.	LPI Inter. Integ.	SDC Inter. Integ.	RCP Seal Integ.	RCP Seal Cooling	AFW	Bleed and Feed	Emerg. AC Power	DC Power	RPS	Manual Scram	Emerg. Borat.
8	Sequoy. Surry Calv. Cl. Zion	Medium high medium medium								average average lower average		average lower lower average	higher average higher average			
9	Sequoy. Surry Calv. Cl. Zion	medium high low low						average average higher average	average average average higher			average lower lower average				
10	Sequoy. Surry Calv. Cl. Zion	low low high low								average average lower average	average average N/A higher					
11	Sequoy. Surry Calv. Cl. Zion	medium medium medium low												average average average	average average average	average lower lower

Plant Specific Design and Operating Insights

This sequence dominates the Zion core damage estimate, is a significant contributor to the Sequoyah frequency[1], yet does not appear in the Surry or Calvert Cliffs risk assessments. The disparity in plant specific contributions (Table 3.4) although somewhat attributable to PRA assumptions regarding the onset of a seal LOCA, indicates major differences in plant response to this initiator. The major variations that influence plant specific contribution to this sequence are:

- This sequence is illustrative of a relative design weakness for some Westinghouse plants. A single cooling system (CCW) provides or supports both reactor coolant pump (RCP) seal cooling modes (thermal barrier cooling and seal injection) and provides essential cooling for the ECCS pumps, which in turn are required for seal LOCA mitigation.

- The Byron Jackson reactor coolant pumps used in the CE plants have a seal configuration (three full pressure seals and a controlled leakoff or a fourth full pressure seal) that provides additional resistance to loss of cooling induced failures beyond that of the typical Westinghouse RCP seal configuration.

- Surry has a cross-connect between the units that enables the second unit's charging pumps to supply seal injection to the Unit 1 RCPs in the event of a loss of CCW. This is limited by the Unit 2 RWST capacity and required makeup from the Unit 1 RWST. Long term mitigation involves RCS depressurization by secondary steaming and LPI/R for injection and long term decay heat removal. At Surry, LPI/R operation is not dependent on CCW for either pump seal or room cooling.

Qualitative Estimate of Sequence Importance

The critical functions for sequence 5 are continued reactor coolant pump (RCP) seal cooling and RCP seal integrity upon loss of all cooling. The former function is generally considered average. Only Surry has a higher assessed RCP seal cooling availability because of the ability to provide seal injection from the other unit's charging pumps. RCP seal integrity is considered average for the Westinghouse plants; Calvert Cliffs has higher assessed RCP seal integrity, as discussed above.

On the basis of the CDF contributions and the relative success estimates for the critical functions, sequence 5 is considered to be highly important (Sequoyah, Zion) unless the aforementioned design features are present. Table 4.1 provides a summary of the assessed importance for sequence 5.

---

[1] See the ** footnote to Table 3.4 which discusses the fact that the Sequoyah PRA was later revised to indicate that the CVCS charging pump bearings are cooled by Service Water, not CCW, so that the pumps could remain operational following loss of CCW.

4.6 Representative Accident Sequence 6: Loss of One 125V DC Bus Initiator

This sequence is initiated by a non-recoverable loss of a 125V DC bus. The DC power system provides control power to various systems. Several precursor studies indicate that there have been several partial losses of DC power at operating nuclear power plants. Approximately one-third of these incidents were caused by the misalignment of breakers during or after system maintenance or surveillances. The remainder of the precursors are due to equipment failures. A loss of one DC bus will typically disable the main feedwater system, a portion of the auxiliary feedwater system and various DC dependent valves, possibly including a power operated relief valve (PORV). This sequence postulates the failure of the remainder of the AFW system and the bleed and feed mode. The failure of secondary heat removal results in core inventory losses due to PORV cycling and subsequent core damage.

The major contributor to this sequence is the failure of the remainder of the AFW system to supply sufficient flow to the steam generators. This typically involves the failure of two additional AFW trains. The major cause is system hardware failures, including pump failure to start, and discharge line faults for both the turbine and motor driven trains. A secondary contributor is the failure to manually start a pump which is procedurally locked out or unable to start due to a malfunction of the autostart logic.

The bleed and feed mode is the decay heat removal method of last resort. Its availability is plant specific, as discussed below.

Plant Specific Design and Operating Insights

The plant specific contributions to representative sequence 6 range from 16% (Calvert Cliffs) to negligible (Surry). The high Calvert Cliffs contribution is indicative of a less diverse decay heat removal capability of CE designs. The Westinghouse plants, by comparison, have a greater assessed AFW availability and also consider the bleed and feed mode. Specific plant design and operating features that contribute to this sequence are:

- The AFW design with regard to the DC power sources is a major determinant of plant vulnerability to sequence 6. Calvert Cliffs, although a 2 unit site, utilizes only two DC trains to support each plant's AFW system. Sequoyah uses all four available DC buses to support AFW. Thus, the Sequoyah contribution is only 2%. Surry's turbine steam inlet valves fail open on loss of DC power. However, although this starts the TDP, if DC power is required for control, it could be tripped due to a high or low steam generator level. Less DC redundancy results in a greater loss of system function due to the initiator alone.

- The Calvert Cliffs AFW system consists of two trains with two turbine driven pumps (one of which is locked out) and a motor driven pump. The single motor driven pump is disabled by the initiating event, which is a loss of its 125V DC bus.

- At Calvert Cliffs, a portion of the AFW discharge line is shared by two pumps. Certain valves can only be disassembled if both pumps are disabled. This results in a higher assessed maintenance unavailability than would normally occur in a system with three separate AFW trains.

- Calvert Cliffs has an AFW pump that is normally locked out and requires a manual start, given that the other two pumps fail to start automatically. A system that requires manual action to perform its function is usually less successful than its automatic counterpart.

- At Calvert Cliffs, the unavailability of one steam generator requires manual adjustment of the AFW flow control valve to increase flow to the remaining steam generator(s) for successful decay heat removal.

Some multiple unit sites have AFW crossties which, although beneficial, have the potential for flow diversion. The concern is a single valve (or multiple valves in parallel) that separates the two units AFW systems. The postulated failure is that the valve is open when indicating closed.

- Main feedwater back leakage causing AFW pump steam binding is a potential common cause failure. Design contributors are normally open pump discharge MOVs, insulated AFW discharge lines and leaking pump discharge check valves. Remedial actions include check valve rework, the removal of the discharge line insulation (to promote steam condensation) and periodic checks of the AFW pump discharge piping temperature.

- The availability of bleed and feed is plant specific. Calvert Cliffs (Ref. 11) does not take credit for this option due to the comparatively low head of the safety injection pumps. The Sequoyah and Surry PRAs (Ref. 4, 12) assume 2 PORVs are required for success. For those plants with DC controlled PORVs, the loss of one 125V DC bus fails one valve, disabling the bleed and feed mode (Sequoyah). The Surry PORVs use AC control power with a DC backup and, hence, do not have this dependency. In the Zion risk assessment (Ref. 13) the plant's bleed and feed capability was re-evaluated and it was concluded that a single PORV is sufficient for success.

- In general, the relatively high availability of the Westinghouse AFW system is responsible for the low Sequoyah contribution to this sequence. The potential availability of feed and bleed at Surry and Zion further reduces plant exposure to the loss of DC bus initiator.

Qualitative Estimate of Sequence Importance

The importance of this sequence is directly related to the assessed availability of the emergency decay heat removal function. The less redundant and diverse designs have higher contributions to representative sequence 6.

If the Westinghouse AFW design represents the average assessed availability, the availability of the Calvert Cliffs AFWS must be lower due to the limited redundancy and the need for manual actions to ensure mission success. The second component of the sequence decay heat removal function is the bleed and feed mode. The Surry design, which requires both PORVs is considered the average. Since the bleed and feed success criteria only require one operable PORV for Zion, the relative availability is higher than average. Bleed and feed is not applicable for Sequoyah or Calvert Cliffs, as discussed above.

The assessed importance for this sequence, as summarized in Table 4.1, is generally low. The sequence is of medium importance for Sequoyah because the loss of one 125V DC bus disables bleed and feed. It is a major contributor to the Calvert Cliffs CDF due to the relatively limited AFW availability and the lack of a bleed and feed capability.

4.7 Representative Accident Sequence 7: Loss of Offsite Power Initiator with Failure of AFW and Bleed and Feed

Sequence Description

Representative accident sequence 7 is initiated by a loss of offsite power (LOOP) with successful operation of at least one source of emergency AC power. Main feedwater is unavailable due to the loss of offsite power. The Auxiliary Feedwater (AFW) system fails due to common mode failures or because of random failures, in concert with the partial system unavailability due to AC power failures. The bleed and feed mode is not successful, generally because of system failures. Since secondary heat removal is not available, the resultant boiloff of primary coolant leads to core damage.

The LOOP initiator is one of the more common operating transients, comprising approximately 21% of all precursors to potential core damage (Refs. 7-10). Although some of these transients are weather or grid related, about 50% of the LOOP precursors are due to human error such as: maintenance errors on the main generator or switchyard breakers, breaker misalignment during or post-maintenance, and equipment operator errors related to breaker operation. In addition, several initiators were caused by station transformer faults.

The subsequent failure of one or more sources of emergency AC power is important because it disables a portion of the Auxiliary Feedwater (AFW) system. The major contributor to this sequence is the failure of the AFW system to provide sufficient flow to the steam generators. Part of the system unavailability is due to the failure of one or more (but not all) EDGs. The remainder of the system fails due to a combination of unrelated faults, such as local failures (primarily valve related) of the AFW turbine steam inlet line or the AFW pump discharge lines and local faults of the turbine driven (TD) pump.

The bleed and feed mode is the option of last resort. The PORV failures can be attributed to failure of a PORV to open on demand or prior closure of the block valve, given a loss of the EDG. The block valve requires AC power to reopen.

Plant Specific Design and Operating Insights

Representative sequence 7 is a loss of the decay heat removal function which is similar to the previous sequence. Once again, Calvert Cliffs is the major contributor due to the limited diversity of the emergency decay heat removal function, as assessed by the PRA. The reason for the Surry contribution is not straightforward and appears to be related to a PRA assumption (assessed PORV availability) in conjunction with postulated common mode failures of the AFW system. The plant specific contributions to the loss of decay heat removal sequences have been presented previously in representative accident sequence 6.

Qualitative Estimate of Sequence Importance

With the exception of the initiator, this sequence is very similar to the previous one. Therefore, it is also of generally low importance. It also is driven by the estimated availability of the decay heat removal function. The estimated availability of the decay heat removal systems is the same with one exception, namely, Sequoyah has been upgraded to an average availability for the bleed and feed mode. In contrast to sequence 6, the LOOP initiator does not prevent the bleed and feed operation.

The estimated importance of sequence 7 is generally low. However, as previously stated, Calvert Cliffs is relatively vulnerable to loss of decay heat removal sequences due to the relatively lower AFW availability and lack of bleed and feed capability. Thus, it has a somewhat higher exposure to representative accident sequence 7.

4.8 Representative Accident Sequence 8: Station Blackout with Loss of AFW

Sequence Description

Sequence 8 is initiated by a loss of offsite power (LOOP), followed by a failure of all emergency diesel generators (EDGs) resulting in a station blackout. Several station blackouts have occurred, but they have been of limited duration. One was during a loss of turbine generator and offsite power startup test. This was caused by an inadvertent isolation of the diesel generator start relays due to a failure to follow the test procedure. The second occurred more recently, during a refueling outage. A truck accident disabled the station transformer. One emergency diesel generator was unavailable due to maintenance and the second failed to start. Sequence 7 provides a discussion of the LOOP initiator. The loss of all AC power results in an immediate failure of all decay heat removal systems except the turbine driven portion of the auxiliary feedwater system. The AFW system subsequently fails resulting in core damage.

The major contributor to this sequence is the failure of emergency AC power. This is dominated by the failures to start or run of all emergency diesel generators (EDGs) or the unavailability of an EDG due to test or maintenance activities with the failure of the remainder to start/run.

The AFW system failures can occur in either the long or short term. Long term failures of AFWS are attributable to station battery depletion, which results in the loss of instrumentation and control power. Short term failures of the AFWS are turbine driven pump or AFW discharge valve failures or the failure to manually open the pump discharge air operated valves.

Plant Specific Design and Operating Insights

All reference plants contribute to this sequence, however, there are CDF variations in Table 3.4 that are attributable to plant design features in the following systems:

Emergency AC Power

- The Zion site has five EDGs, two dedicated diesels per unit plus a fifth swing diesel. A single diesel at each unit is sufficient to avert a blackout.

- Sequoyah has the capability to supply emergency power between units via a shutdown utility bus.

- In contrast the Surry site has 3 EDGs (one dedicated per unit, one swing EDG). Each unit requires at least one out of the three EDGs to prevent SBO. Multiple EDGs do not necessarily reduce the common mode failure potential. However, more EDGs means that random diesel faults or maintenance unavailability becomes less critical, leading to a higher success rate. Calvert Cliffs has a similar design configuration with 3 EDGs for the two units.

DC Power

- The Sequoyah DC power configuration consists of four independent trains with multiple hard wired cross feeds. A fifth battery can be connected to any bus in about ten minutes. In addition, the DC power for the Unit 1 AFW system is normally supplied by the Unit 2 DC buses. These are likely to remain operable unless there is a simultaneous SBO at both units.

- Calvert Cliffs has a DC power design that enables the dedicated Unit 2 EDG to charge two of the four shared DC buses without operator action.

- The DC power buses appear to be completely independent between the two Surry units. There does not appear to be a simple mechanism to allow the dedicated EDG at Unit 2 to charge a Unit 1 DC bus.

AFW

- The AFW design insights are the same as discussed previously for sequence 6.

Qualitative Estimate of Sequence Importance

Sequence 8 presents a complex interaction between the decay heat removal function (AFW) and the supporting emergency power systems (AC and DC). The AFW system can fail in the short term due to intra-system faults or in the long term as a consequence of station battery depletion. The estimated availability of the AFW system has been discussed in sequence 6.

The Emergency AC (EAC) power system availability is deemed "average" if more than two diesel generators must fail to start to cause a station blackout. At Surry and Calvert Cliffs, there are a total of three EDGs for both units. One is shared between units (swing diesel). If a LOOP occurs and two EDGs are unavailable at the time, one unit will not have AC power available.

At Sequoyah, there are four EDGs for two units. If two EDGs fail at a single unit, AC power from the opposite unit can be supplied through a shutdown utility bus.

Zion has a total of five EDGs for both units. One is a shared swing diesel. In order for a loss of AC power (station blackout) to occur at any one unit, both of the EDGs dedicated to that unit must fail, and the swing diesel must fail as well.

The reference design for the DC power system is a single unit plant site, or a multi-unit site without hardwired cross feeds between units (Surry, Zion). Sequoyah and Calvert Cliffs have system cross-ties between units, resulting in a higher estimated availability.

Representative sequence 8 is of medium importance, except at Surry where it is highly important. This sequence shows the impact that support systems can have. Despite a relatively good AFW availability, the sequence contribution is higher than normal due to limitations in the emergency power systems.

4.9 Representative Accident Sequence 9: Station Blackout with Reactor Coolant Pump Seal LOCA

Sequence Description

Sequence 9 is also initiated by a station blackout. The loss of all AC power disables all primary system injection, as well as reactor coolant pump (RCP) seal cooling. Unlike sequence 8, the AFW system provides decay heat removal. An RCP seal LOCA occurs, resulting in the loss of the primary system inventory and the onset of core damage.

The major contributor to this sequence is the failure of all emergency AC power. This is dominated by the failure to start/run of all emergency diesel generators (EDGs) or the unavailability of one EDG due to test or maintenance, coincident with the failure of the remaining units.

The loss of all AC power results in a loss of cooling to the RCP seals. The RCP LOCA accelerates the loss of primary coolant and limits recovery measures to approximately one hour. Major recovery actions are the recovery of AC power and successful restoration of HPI component cooling.

Plant Specific Design and Operating Insights

As shown in Table 3.4, the plant specific vulnerability can vary greatly depending on certain design features. The major influences on sequence importance are the degree of failure resistance of the RCP seals under loss of cooling conditions (see sequence 5), the emergency AC power availability to support seal cooling (sequence 8), and the seal cooling configuration for multi-unit sites, discussed below.

- The Zion CCW and Service Water (SW) systems are shared between the units. In addition, all five EDGs can power both a CCW and a SW pump. This configuration permits the continued operation of the CCW system at both units, despite the loss of all AC power (3 EDGs) at one unit. This capability is why Zion does not contribute to sequence 9.

- Sequoyah also has a shared CCW system. However, the thermal barrier booster pumps are powered by the same unit's EDGs (i.e., no crossfeeds). Although the CCW system could be available during an SBO, RCP seal cooling would not be maintained due to a loss of power to the booster pumps.

Qualitative Estimate of Sequence Importance

The plant specific resistance to representative accident sequence 9 depends upon the availability of emergency AC (EAC) power. Surry, although similar to Sequoyah and Zion in the other critical functions, has less EAC redundancy. This is the primary reason for the high Surry contribution to this sequence.

Calvert Cliffs has a similar EAC configuration, but, its higher degree of resistance to RCP seal failures results in a low contribution to this sequence. Table 4.1 provides a summary of the estimated importance for representative accident sequence 9.

4.10 Representative Accident Sequence 10: Loss of PCS Initiator (or Transient Followed by Loss of PCS) with Loss of AFW

Sequence Description

Sequence 10 is a loss of the Power Conversion System (PCS) initiator (or a transient followed by a loss of PCS) with the subsequent failure of the AFW system. As a result of the loss of decay heat removal, the primary system overheats. The associated system pressurization causes PORV cycling, a loss of system inventory and subsequent core damage.

The precursor (Refs. 7-10) studies were reviewed to determine major sources of PCS failures in operating nuclear power plants. Main feed pump trips comprised over 25% of the total number of PCS failures. These included valid, spurious or operator induced low suction pressure trips, feed pump turbine controller failures and gradual losses of condenser vacuum or hotwell level in which the operators did not believe the instrument readings. Steam dump valve closure failures, primarily due to positioner linkage problems, contributed approximately 15%. The remainder of the loss of PCS precursors is fairly evenly divided among condensate pump trips, feedwater recirculation, control and bypass valve malfunctions, feedwater controller failures and miscellaneous contributors, including multiple stuck open relief valves and main turbine trips which induced PCS isolations.

The loss of the Auxiliary Feedwater (AFW) system is the main contributor to this sequence. The majority of the system unavailability is due to operator failures to manually start either a locked out pump or a pump with a disabled auto start circuit. Hardware failures include steam admission suction valve and pump local faults. The unavailability of a pump or a pump discharge valve due to maintenance activities is also a contributor.

Although the plant specific input used to develop this representative sequence did not consider it, the bleed and feed mode could also be used for decay heat removal. The major contributors to the failure of feed and bleed are PORV or block valve faults and human error.

Plant Specific Input and Sequence Ranking

This sequence postulates a failure of the decay heat removal function and is generally considered to be of relatively low risk importance at most plants, as depicted in Table 3.4. Calvert Cliffs is the exception, for a variety of reasons. The lower assessed availability of the AFW system and the lack of bleed and feed has been previously discussed in sequence 6. An additional relative susceptibility is that the two major decay heat removal systems (main and auxiliary feedwater) have a total or partial dependence on a single vital AC power inverter. This dependency essentially doubles the Calvert Cliffs core damage frequency contribution due to loss of main feedwater.

The Westinghouse plant PRAs examined do not indicate any significant contributions to this sequence because of the relatively high availability of AFW and bleed and feed. In addition, motor driven main feedwater pumps reduce plant vulnerability to sequence 10 even further.

Qualitative Estimate of Sequence Importance

This sequence postulates a loss of decay heat removal and is similar in progression to sequence 7. The plant specific availability estimates for AFW and bleed and feed are the same. As previously indicated, the Westinghouse plants have a relatively lower exposure to loss of decay heat removal sequences. The Calvert Cliffs design contribution to this sequence type is relatively more significant, for the reasons previously discussed.

4.11 Representative Accident Sequence 11: ATWS with Failure of Emergency Boration

Sequence Description

This sequence is initiated by a transient from high power followed by an RPS failure to automatically scram the reactor. The attempts to manually scram are not successful and emergency boration also fails.

The initiator is a transient such as an MSIV closure, partial loss of feedwater, feedwater flow increase or a loss of reactor coolant system (RCS) flow that results in a turbine trip and PCS runback. The mismatch between core power production and secondary loop heat removal results in RCS coolant loss through the PORVs. Core uncovery and damage occur in forty minutes or less. The Salem nuclear power plant experienced two RPS failures to trip on the automatic trip signals, but manual trip was successful. The failures were caused by malfunctions of the reactor trip breaker undervoltage attachments.

The failure to manually scram the reactor is caused by operator error or hardware failures of the control rods or drives that prevent insertion. The failure of emergency boration is dominated by operator failure to initiate injection, while system hardware faults have a smaller contribution.

Plant Specific Design and Operating Insights

Table 3.4 includes depicts plant specific contributions to sequence 11 that vary from 27% (Calvert Cliffs) to less than 1% for Sequoyah. No ATWS sequence information was available for Zion in References 13 or 14. The Calvert Cliffs contribution is driven by the decision not to credit manual scram in the risk assessment. When this conservatism is eliminated, the sequence contribution is comparable to Sequoyah or Surry.

Given the high reliability of RPS, with credit for manual scram, the design differences of the emergency boration function appear to have a modest influence on the plant specific contributions to sequence 11.

The operator actions required to initiate boric acid injection are dependent on system design. Some plants have an in-line boric acid injection tank with redundant valving that is an integral part of the charging system/high pressure injection lineup. The hardware failure for this configuration is negligible. Injection failure is attributable to the failure to manually activate the system.

Other plants utilize one or two boric acid pumps discharging through a common, normally closed, high flow line to the charging pump suction header. Operator action is required to start a second pump (or switch a single operating pump to fast speed operation) and open the normally closed MOV. This configuration is more vulnerable to hardware failures related to the use of a single, normally closed MOV and/or the system success criteria that require two out of two boric acid pumps to operate.

Qualitative Estimate of Sequence Importance

From the foregoing discussion, the reference plants (for which accident sequence information is available) have an estimated medium importance for representative accident sequence 11.

Section 4 has provided a discussion of the representative accident sequences and, in particular, the effect of design and operating features on reference plant vulnerability. The next section prioritizes the individual component failures and human actions that comprise each sequence and also examines the impact of plant specific design and operating variations on that ranking.

5. IDENTIFICATION OF RISK IMPORTANT SYSTEMS, COMPONENTS, AND HUMAN ACTIONS

In a PRA, plausible accident scenarios are chosen for analysis. The accident scenario begins with an initiating event such as loss of offsite power, which is then referred to as the **initiator**. Subsequent system failures such as failure of the emergency diesel generators to function can occur due to component failures or unavailabilities due to test or maintenance outages, or due to human errors. These individual failures are referred to as **basic events**. The scenario proceeds with additional failures occurring until core damage occurs. The overall accident scenario leading to core damage is then referred to as an **accident sequence**.

Each accident sequence is evaluated by assigning a probability of occurrence to each basic event, which is then referred to as the **basic event probability**. The result is that each accident sequence has a frequency of occurrence which represents its contribution to the total frequency of core damage. Hence, the logical sum of all the **accident sequence frequencies** represents the **total core damage frequency**. The number of plausible accident scenarios can be 100 or more. However, only a portion of these scenarios, or accident sequences, account for the bulk of core damage frequency. The latter sequences are referred to as the **dominant accident sequences**.

The term logical sum refers to the need to avoid multiple counting of accident sequence failure combinations, referred to as **cutsets** in PRA terminology, which appear more than once in the core damage frequency summations. Only the minimum number of failure combinations, or **minimal cutsets**, should be accounted for.

The term risk can vary in application. That is, one can calculate the **risk of core damage**, which may have no adverse effects on human beings, or the **risk of containment failure**, which again may or may not affect human beings. Ideally, one is interested in the risk of radioactivity releases to the environment affecting the short term or long term health of human beings. Hence, the term **risk of health effects** is also used. The complexity and uncertainty of the calculational models, as well as the need for detailed site specific information, greatly increase as containment failure modes and health effects are considered. For the purposes of the methodology presented in this report, the detailed risk insights that would be so developed would have limited generic applicability. This report focuses on core damage frequency as an approximation of risk. (In a stric sense, only the frequency of core damage is considered in this report, not the risk of core damage, because risk implies the probability of health effects on human beings or other parts of the environment.)

In the discussion which follows, the method by which the contributing basic events that comprise the accident sequence cutsets are prioritized is explained. This prioritization process results in a numerical value, or **importance measure**, for the basic events. The **basic event importance measure** calculations can be organized in a different fashion so that **plant system importance measures** can be generated.

5.1 Calculation of Average System and Basic Event Importances

A single accident sequence can be composed of several hundred cutsets. To maintain the desired importance measure calculations at a reasonable level, only the cutsets that appeared in the top 80% of a plant specific sequence's probability of core damage (its CDF contribution) were considered. If this was still not practical, only those cutsets greater than, or equal to, 1% of the sequence's CDF contribution were considered. For each plant specific dominant accident sequence, either the Inspection Importance or the Fussell-Vesely Importance was calculated for all of the basic events appearing within the sequence boundaries defined above.

The **Inspection Importance** of a given basic event is the summation of the CDF contributions of all the cutsets in which the basic event appears, either within a particular accident sequence or among all of the plants accident sequences upon which the total CDF is calculated. The **Fussell-Vesely Importance** may be defined as the Inspection Importance divided by a constant value, usually the total CDF, or else the CDF contribution of the particular accident sequence. The importance measures which were obtained in this manner were normalized, so that the summation of these normalized basic event importances equals 100% for each sequence.

In reality, each of the representative sequences encompasses more than one plant specific accident sequence. That is, there are multiple plant specific accident sequences associated with a representative accident sequence. As a result, an average basic event importance was calculated for each basic event by taking the summation of all the normalized basic event values for that same event, and then dividing by the total number of contributing sequences.

Mathematically, the above discussion can be represented as follows:

$$I_\ell^P = \frac{I_\ell^I}{\sum_{i=1}^{m} I^I(i)} \qquad (5\text{-}1)$$

where

I_ℓ^I = the Inspection Importance of the ℓ component for a plant specific sequence

m = the number of basic events in a plant specific sequence

I_ℓ^P = the normalized importance for basic event ℓ of a plant specific sequence

Each of the normalized basic event importances, I_ℓ^P, are then substituted into the following equation

$$I_\ell^A = \frac{1}{n} \sum_{i=1}^{n} I_\ell^P(i) \qquad (5\text{-}2)$$

where I_ℓ^A = the average basic event importance for event ℓ of a representative accident sequence.

n = the number of plant specific sequences associated with a representative accident sequence.

For example, refer to Table 5.1, Representative Sequence 1, the human error of High Pressure Injection/Recirculation "Failure to switch from RWST to the containment sump via the LPR system including failure to stop pumps on RWST lo-lo alarm."

The plant specific contributors to Representative Sequence 1 are:

Plant	Specific Sequence No.	Total No. of Sequences
Sequoyah	1,3,4,6	4
Calvert Cliffs	3,4,15	3
Surry	2,10,13,14,19	5
Zion	2	1
		n=13

The basic event Inspection Importance for the particular human error, event ℓ, is:

Plant	Specific Sequence No. Containing Event ℓ	Normalized Inspection Importance for Event (I_ℓ^P)
Sequoyah	1	42
	6	44
Calvert Cliffs	4	1
Zion	2	15
		$\Sigma I_\ell^P = 102$

The average basic event importance, I_ℓ^A, is then:

$$I_\ell^A = \frac{1}{n} \sum I_\ell^P = \frac{1}{13}(102) = 8$$

It should be noted that the Surry, Sequoyah (Ref. 4, 12), and Calvert Cliffs (Ref. 11) PRAs were selected for the system and event importance calculations for each representative sequence. Locating an additional risk assessment that contained dominant accident sequence cutsets was difficult. After evaluation of alternatives, it was decided to include the NRC-developed System Analysis and Risk Assessment (SARA) system (Ref. 14) for Zion. The SARA sequence probabilities showed good correlation to the values published in NUREG/CR-4550, Vol. 7 (Ref. 13), for the sequences of interest.

5.2 Development of Plant Specific Modifiers

In the example in Section 5.1 above, it was shown how the average basic event importances provided in Table 5.1 were calculated. The next step is to illustrate how the average event importances should be adjusted for application to plants. The adjustment factors are referred to as Plant Specific Modifiers (PSM).

A total of 65 modifiers are provided in Table 5.1. They are intended to accommodate the various differences in design and level of redundancy in Westinghouse and CE plants not subjected to a PRA. The events in Table 5.1 are cross-referenced to the applicable modifiers. Plant specific basic event importances for plants not subjected to a PRA can be derived using these modifiers. These modifiers reflect, in an approximate manner, the deviations from the four reference plants (Sequoyah, Surry, Calvert Cliffs and Zion).

As an example, for the same basic event mentioned in Section 5.1, PSM No. 8 is cross-referenced in Table 5.1 The factor of 3 (PSM No. 8) was developed in the following way. In the Sequoyah PRA, there were four contributing sequences to Representative Sequence No. 1., i.e., Nos. 1, 3, 4, and 6. Of these, only sequence Nos. 1 and 6 contained the basic event. The Normalized Inspection Importance for the basic event in each of those two sequences was 42 and 44, respectively. Hence, the Average Inspection Importance for this event, considering only Sequoyah is:

$$I_i^A = \frac{42+44}{4 \text{ sequences}} = 21$$

versus the average for all plants, $I_i^A = 8$. The intent of the plant specific modifier (PSM) is to approximate the contribution this basic event would make in a plant with a design configuration of its HPI and HPR systems similar to Sequoyah's. Hence, the applicable PSM (No. 8) is:

$$PSM = \frac{21}{8} = 3$$

PSMs have only been provided for basic events in which plant design or operational variations have a strong influence, either positively or negatively, on the CDF contribution of a representative sequence.

To summarize, Table 5.1 presents the basic events for each representative accident sequence, including the associated average importance estimates. These importance values can be used to rank the sequence contributors on a relative basis only. For example, a value of eight is considered to be more risk significant than an estimate of two, but not necessarily four times as important. In addition, small differences are not considered to be significant.

The average importance values are just that, a composite of the plant specific accident sequence information. As such, the accident contributors are identified, but the prioritization, based on average importance, may de-emphasize the risk significance of certain plant specific variations, hence, the use of the PSMs.

5.3 Ranking of the Basic Events

Thus far, the methodology has had an accident sequence emphasis, meaning that failure descriptions and basic event rankings were presented within the framework of a sequence. From a PRA perspective, the accident sequence approach provides the context for the examination of component failures, human actions, and their interrelationships. However, it is more convenient to organize the important events by plant activities. Appendix A presents an inspection matrix which is a plant activity based organization of the basic events associated with all eleven representative accident sequences. As before, risk significant design and operating variations can be incorporated to provide a plant specific prioritization of systems, components, and human actions.

Table 5.1

Representative Accident Sequence Importance Summary

Representative Accident Sequence 1:

Small or Medium LOCA with Failure of High Pressure Injection or Recirculation

Event Description	Average Importance[1,2]	Plant Specific Modifier
Initiator		
Small/Medium LOCA Initiator	43	
High Pressure Injection/Recirculation		7
• Human Error		
Failure to switch from RWST to the containment sump via the LPR system including failure to stop pumps on RWST lo-lo alarm	8	8
• Valves		
Failure of common HPI discharge valve(s) to open (including common cause)	8	9
Failure of common HPI suction valve (from RWST) to open, including check valves	2	
Plugging of manual valve in the common HPI suction line	2	
Failure of mini flow valve to open	4	
Failure of HPR suction valve(s) (including common cause)	5	
Safety injection mini flow valve fails to close. Interlock fails pump suction valves from LPR.	<1	
	Valve subtotal = 21	
• Pumps		
Local fault of pump(s) (incl. common cause)	2	
Failure of control cable to pump	<1	
Failure of pump breaker to close	<1	
Pump in maintenance	<1	
	Pump subtotal = 2	
	HRI/R total = 31	
Low Pressure Recirculation		11,12,13
• Human Error		
Failure to stop LP/pumps if mini flow valve doesn't open/failure to restart pump for recirculation	1	14
• Pumps		
Pump(s) fail to start (incl. common cause)	4	15
Pump fails to run	1	
• Valves		
LPI mini flow valve(s) fail to open (incl. common cause)	4	14
Failure of LPR suction valve(s) to open	4	15
Failure of LPI suction valve to close (from RWST)	1	15
	Valve subtotal = 9	
Containment sump plugging	1	21
	LPR total = 16	

[1,2] See General notes 1 and 2, repectively in the listing of Plant Specific Modifiers which accompanies this table.

Table 5.1

Representative Accident Sequence Importance Summary (Cont'd)

Sequence 1: (Cont'd)

Event Description	Average Importance[1,2]	Plant Specific Modifier
Component Cooling Water		60
• Human Error		
Failure to manually align standby train after failure of operating loop	1	
• Pumps		
CCW pump(s) fails to run (incl. common cause)	<1	62
• Valves		
Local fault of any CCW valve that disables all ECCS pump coolers	<1	
Local fault of standby HX bypass valve	1	
Local fault of standby HX outlet valve	<1	
	CCW total = 2	
Service Water		60
• Valves		
Failure of any SW valve which stops SW flow to CCW HX	1	61
• Pumps		
Common cause failure of SW pumps that ultimately cool the HPI pumps	<1	
Common cause failure of HPI cooling water strainers (lube oil cooling/seal injection)	1	
	SW total = 2	
Room Cooling		
Electrical failures (power cable/breaker) disable HPR pump room cooling	3	65
Failure of SW valve disables HPR pump room cooling	1	65
	Room Cooling total = 4	
RWST		
• Human Error		
Miscalibration of RWST level sensors due to common cause fails manual or auto realignment of high pressure ECCS	3	
Operator fails to remove refuel drain plugs after refuel outage	1	22
	RWST total = 4	

[1,2] See General notes 1 and 2, repectively in the listing of Plant Specific Modifiers which accompanies this table.

Table 5.1

Representative Accident Sequence Importance Summary (Cont'd)

Representative Accident Sequence 2:

Medium or Large LOCA with Failure of Low Pressure Recirculation

Event Description	Average Importance[1,2]	Plant Specific Modifier
Initiator		
Medium/Large LOCA	51	
Low Pressure Recirculation		11,16
• Human Error		
Failure to switch from cold to hot leg LPR	3	
Failure to successfully switch from LPI to LPR including valve alignment errors	20	17
	Human Error subtotal = 23	
• Valves		
LP hot leg recirc. disch. valve fails to open	1	
LPR sump suction valve(s) fail to open	7	15
Failure of RWST pump suction valve to close	7	15
Pump discharge crossover valve fails to close	<1	
Cold leg isolation valve(s) fail to close	4	
	Valve subtotal = 19	
• Pumps		
Low pressure pump(s) fail to run (incl. common cause)	4	15
	Pump subtotal = 4	
	LPR total = 46	
RWST		
• I&C		
Common cause miscalibration of the RWST level sensors	4	

[1,2] See General notes 1 and 2, repectively in the listing of Plant Specific Modifiers which accompanies this table.

Table 5.1

Representative Accident Sequence Importance Summary (Cont'd)

Representative Accident Sequence 3:

Medium or Large LOCA with Failure of Low Pressure Injection

Event Description	Average Importance[1,2]	Plant Specific Modifier
Initiator		
Medium/Large LOCA	51	
Low Pressure Injection		10
• Human Error		
Failure to stop pumps if mini flow valve fails to open	1	18
Failure to realign system after testing	5	19
• Valves		
LPI mini flow valve(s) fail to open (incl. common cause)	2	18
• Pumps		
LPI pump(s) fails to start (incl. common cause)	11	
LPI pump(s) fails to run (incl. common cause)	3	
	Pump subtotal = 14	
	LPI total = 22	
Accumulators		20
• Injection Failure (including check valve failure to open/MOV plugging)	27	

[1,2] See General notes 1 and 2, repectively in the listing of Plant Specific Modifiers which accompanies this table.

Table 5.1

Representative Accident Sequence Importance Summary (Cont'd)

Representative Accident Sequence 4:

LOCA Outside Containment (ISLOCA)

Event Description	Average Importance[1,2]	Plant Specific Modifier
Initiators		
Low Pressure Coolant Injection Lines		23, 24, 25
• Transfer open of 1 check valve followed by a rupture of the second interface valve	47	
• Failure of one valve to close on repressurization followed by rupture of the second	2	26
• Rupture of interface valves	1	
Shutdown Cooling Lines including	34	27, 28
• Both interface valves rupture • Downstream valve transfers open, upstream valve ruptures		
Recovery Action		
• Operator failure to isolate LPI interfacing LOCA	16	29

[1,2] See General notes 1 and 2, repectively in the listing of Plant Specific Modifiers which accompanies this table.

Table 5.1

Representative Accident Sequence Importance Summary (Cont'd)

Representative Accident Sequence 5:

Loss of all CCW Initiator

Event Description	Average Importance[1,2]	Plant Specific Modifier
Initiators		30, 31, 32
• Failure of CCW due to a pipe rupture	49	
• Common cause failure of running CCW pumps	25	62
CCW System		62
• Pumps		
Standby pump(s) in maintenance	<1	
Standby pump(s) fail to start	18	62
Standby pump(s) fail to run	7	62

[1,2] See General notes 1 and 2, repectively in the listing of Plant Specific Modifiers which accompanies this table.

Table 5.1

Representative Accident Sequence Importance Summary (Cont'd)

Representative Accident Sequence 6:

Loss of One 125V DC Bus Initiator

Event Description	Average Importance[1,2]	Plant Specific Modifier
Initiator		
Loss of a 125V DC bus	31	
AFW System		33
• Human Error		
Operator fails to manually start locked out pump	7	34
Operator fails to manually start pump, given auto start failure	3	
Operator fails to restore turbine driven pump from test	<1	
Failure to crossfeed AFW from another unit of a multiple unit site	3	
Operator fails to increase flow to SG given unavailability of the other SG	1	35
Failure to restore AFW turbine driven pump discharge valve after test	<1	
	Human Error subtotal = 14	
• Pumps		
Motor driven (MD) AFW pump fails to start	15	36
MD pump fails to run	1	36
Turbine driven (TD) pump fails to start/run	17	
TD pump in maintenance	3	
TD pump in test	<1	
	Pump subtotal = 36	
• Valves		
Throttle/Trip valve fails to open (valve faults in steam admission line)	2	
AFW FW valve in maintenance that disables two AFW pumps	1	37
Local fault of valve in MD pump disch. to SG	12	36
Local fault of valve in TD pump disch. to SG	2	
	Valve subtotal = 17	
	AFW total = 67	
Safeguards Actuation Signals		
Failure of AFW auto actuation	3	
Feed and Bleed Mode		42
PORV fails to open		43
Bleed and feed human error		43

[1,2] See General notes 1 and 2, repectively in the listing of Plant Specific Modifiers which accompanies this table.

Table 5.1

Representative Accident Sequence Importance Summary (Cont'd)

Representative Accident Sequence 7:

Loss of Offsite Power Initiator with EDGs Operable, Loss of AFW

Event Description	Average Importance[1,2]	Plant Specific Modifier
Initiator		
Loss of offsite power	26	
AFW System		33
• Human Error		
Undetected flow diversion	4	38
Operator fails to start locked out pump	12	34
Operator fails to manually start given auto start failure	<1	
	Human Error subtotal = 16	
• Valves		
Undetected FW back leakage through pump discharge check valves causes steam binding	3	39
Local fault of AFW suction valve from the CST fails all operating AFW pumps	2	40
Local fault of valve in turbine driven (TD) AFW pump steam admission line	3	
Maintenance of valve in an AFW pump feedwater line disables two pumps	5	37
Failure to provide AFW feedwater flow due to faults in motor driven (MD) discharge line pipe segment (local faults in the pump discharge valves)	<1	
Failure to provide AFW flow due to faults in turbine driven discharge line pipe segment (local faults in the pump disch. valves)	<1	
	Valve subtotal = 15	
• Pumps		
Local fault of AFW TD pump	6	
Local fault of MD pump	2	
Local fault of MD pump power breaker	<1	
TD pump undergoing maintenance	4	
	Pump subtotal = 12	
	AFW total = 43	
Emergency AC Power		
EDG fails to start on demand	17	
EDG unavailable due to maintenance	2	
EDG fails to continue to run	6	
EDG not returned to service from test	<1	
	Emergency AC Power subtotal = 25	

[1,2] See General notes 1 and 2, repectively in the listing of Plant Specific Modifiers which accompanies this table.

Table 5.1

Representative Accident Sequence Importance Summary (Cont'd)

Sequence 7: (Cont'd)

Event Description	Average Importance[1,2]	Plant Specific Modifier
Bleed and Feed Mode		42
Failure of a PORV to open on demand	6	44
PORV block valve closed	1	45
	Bleed and Feed subtotal = 7	
Vital Buses/Inverters		
Local fault of inverter fails auto actuation AFW pump	1	

[1,2] See General notes 1 and 2, repectively in the listing of Plant Specific Modifiers which accompanies this table.

Table 5.1

Representative Accident Sequence Importance Summary (Cont'd)

Representative Accident Sequence 8:

Station Blackout with Loss of AFW

Event Description	Average Importance[1,2]	Plant Specific Modifier
Loss of Offsite Power Initiator	22	
AFW System		
• Human Error Failure to manually open TD pump discharge valves	1	41
• Pumps AFW TD pump fails	15	
• Valves Fault in turbine driven discharge pipe segment, primarily due to valve failure	1 AFW subtotal = 17	
Emergency AC Power		
EDG(s) fails to start (incl. common cause)	16	
EDG(s) fails to continue to run (incl. common cause)	12	
EDG unavailable due to test or maint.	8	
	Emergency AC Power Total = 36	
Recovery Action		
Failure to recover AC power	25	46

[1,2] See General notes 1 and 2, repectively in the listing of Plant Specific Modifiers which accompanies this table.

Table 5.1

Representative Accident Sequence Importance Summary (Cont'd)

Representative Accident Sequence 9:

Station Blackout with RCP Seal LOCA

Event Description	Average Importance[1,2]	Plant Specific Modifier
Loss of Offsite Power Initiator	26	
Emergency AC Power		
EDG(s) fails to start (incl. common cause)	27	
EDG(s) fails to continue to run (incl. common cause)	13	
Test & Maint. unavailability of EDG	9	
	Emergency AC Power Subtotal = 49	
Recovery Actions		
• Failure to recover AC power	27	46

[1,2] See General notes 1 and 2, repectively in the listing of Plant Specific Modifiers which accompanies this table.

Table 5.1

Representative Accident Sequence Importance Summary (Cont'd)

Represe itative Accident Sequence 10:

Loss of PCS Initiator (or Transient Followed by Loss of PCS) with Loss of AFW

Event Description	Average Importance[1,2]	Plant Specific Modifier
Initiator		
Loss of PCS transient (or general transient followed by loss of PCS)	27	
AFW System		33
• Human Errors		
Failure to manually start locked out turbine driven (TD) pump	9	34
Failure to manually start motor driven (MD) pump, given auto start failure	17	47
Failure to restore TD pump disch. valve from test	<1	
	Human Error subtotal = 26	
• Valves		
Local fault of AFW suction valve	5	
Local fault of steam admission valve	6	
Maint. of steam admission valve	<1	
Maint. of pump disch. valve fails multiple pumps	1	37
	Valve subtotal = 12	
• Pumps		
AFW TD pump local fault	7	
AFW TD pump in maintenance	5	
AFW TD pump in test	1	
AFW MD pump local fault	2	
AFW MD pump in maintenance	<1	
AFW MD pump circuit breaker fault	2	
	Pump subtotal = 17	
• AFW Logic		
Local fault of AFW logic system fails to actuate MD pump and/or one TD pump steam valve	1	
	AFW total = 56	
Vital AC Power		
Loss of vital AC bus fails AFW TD pump steam admission valve and MD pump	17	47
Safeguards Actuation Signals		
Fault in ESFAS sequencer fail auto actuation of MD pump	<1	
Feed and Bleed Mode		42, 43

[1,2] See General notes 1 and 2, repectively in the listing of Plant Specific Modifiers which accompanies this table.

Table 5.1

Representative Accident Sequence Importance Summary (Cont'd)

Representative Accident Sequence 11:

ATWS with Failure of Emergency Boration

Event Description	Average Importance[1,2]	Plant Specific Modifier
Trans'ent Event Requiring a SCRAM	28	
Failure of RPS	28	
Failure of Manual SCRAM	17	
Emergency Boration		
• Human Error Failure to perform (initiate) emergency boration	23	
Hardware		
Failure of boric acid transfer pump to provide sufficient flow	2	57, 58
Maintenance of charging pumps	2	56
Valves		
Local fault of one valve results in system failure Control circuit fault of one valve disables system Power cable to one valve fails disabling system	3	59

[1,2] See General notes 1 and 2, repectively in the listing of Plant Specific Modifiers which accompanies this table.

Plant Specific Modifier (PSM) Notes for Table 5.1

General

1. The average importance is a composite of the input PRAs. These values can be used to prioritize the failure modes on a relative basis. Small differences in importance values are not significant.

2. The average importance estimates should be used unless, as indicated elsewhere in these notes, plant specific design or operating features exist that can significantly alter the average importance estimates. In that case, the appropriate note will provide guidance to revise the average importance value to reflect a plant specific attribute.

3. The estimated importance for sequence 7 has been revised to "low" based on the conservative PORV availability assumption used in the Surry PRA.

4. Surry has motor driven main feedwater pumps which, unlike turbine driven pumps, are expected to be available after MSIV closure, loss of turbine bypass etc. This reduces the importance of sequence 10 still further.

5. No ATWS information is available for Zion in NUREG/CR-4550 vol. 7 or the SARA Code for sequence 11.

6. The Calvert Cliffs PRA (NUREG/CR-3511) did not credit manual scram. When this conservatism is eliminated, the relative importance of sequence 11 is similar to Surry or Sequoyah.

High Pressure Injection/Recirculation

7. High pressure injection/recirculation (HPI/R) success criteria for a small or intermediate LOCA is generally the continued flow from one of four (or three) high pressure pumps to the RCS given successful low pressure system operation (if required).

8. This is an average importance value, based on input from the surrogate PRAs. If the plant HPI/R design is known it can be modified as follows:

   - For an ECCS design that requires operator action to manually realign the high pressure or low pressure injection system from the injection mode to the recirculation configuration. In conjunction with a large dry containment, multiply the average importance value by a factor of 2.

   - For a similar ECCS design, but with an ice condenser containment, multiply the average importance value by a factor of 3.

   - This failure mode is not critical for ECCS designs that automatically align to the high pressure recirculation mode. Replace the average importance value with a value of 1.0 to reflect manual realignment after the automatic function fails.

9. The importance of this failure mode is directly related to the number of RCS injection pathways and if the injection valves are required to open for system success. The configuration under consideration (Surry) has a single system (charging) for HPI and two normally closed MOVs in

parallel, which are automatically opened by a safety injection signal. As a recovery, another injection pathway could be remote manually opened. But in general, this HPI design is more susceptible to injection valve failures. To reflect this, quadruple the average importance value for discharge configurations that resemble Surry. In contrast, the Calvert Cliffs configuration has eight injection MOVs with only one required for successful mitigation. Although these valves are normally closed, failure of all 8 is unlikely and this failure mode can be neglected.

Low Pressure ECCS

10. Successful low pressure injection generally requires the operation of one out of two trains. Room cooling is not required during the injection phase, but pump seal and lube oil cooling are usually necessary.

11. Low pressure recirculation (LPR) success criteria are generally one out of two trains supplying makeup to the high pressure ECCS (small LOCA) or to the RCS (large LOCA). Pump room cooling and pump cooling are usually required, making component cooling water and service water vital for successful LPR.

12. For small and medium LOCAs, Low Pressure Injection/Recirculation (LPI/R) is a support system for HPR at Westinghouse plants. As such, the failure of the low pressure recirculation can result in core damage even for small pressure boundary failures. The Combustion Engineering (Calvert Cliffs) design does not exhibit this dependency, and LPR failures should be omitted.

13. Among the Westinghouse units, low pressure recirculation is even more important for plants with ice condenser containments. The free volume is smaller than in large dry containments causing faster pressurization which, in conjunction with a lower spray setpoint, activates the sprays earlier. This in turn, results in an earlier need for recirculation. It has been estimated that a small LOCA at Sequoyah could require a switchover to the recirculation mode in about 80 minutes following accident initiation or 20 minutes following containment spray actuation. For the same size break, a large dry containment would not require recirculation switchover for several hours. This could give the operator time to lower the RCS temperature, depressurize and transfer to closed cycle shutdown cooling. The accelerated timing for the smaller ice condenser containment design does not allow this.

14. This importance estimate (sequence 1) is based on normally closed low pressure ECCS minimum flow valves. Neglect for normally open valves with out of position annunciation in the control room.

15. Multiply by a factor of two for ice condenser containments. See also note 13.

16. This sequence is not applicable to Calvert Cliffs. The CE design uses high pressure recirculation to mitigate all break sizes. The RWST low level signal causes high pressure ECCS switchover and stops the low pressure ECCS injection which is generally locked out by the recirculation signal.

17. If manual realignment of the LP ECCS pump suction from the RWST to the containment sump is required, multiply this average importance value by a factor of 2. If the plant design has automatic switchover, reduce the importance estimate to 1 to account for the need for manual realignment, only if the automatic function fails.

18. Multiply this importance value by a factor of three (sequence 3) if the plant has a normally closed mini flow valve configuration where the valves must open on system initiation to prevent pump damage at high RCS pressures. Not applicable for normally open mini flow valves unless valve mispositioning is unlikely to be detected.

19. If there is no provision for the detection of system misalignments, multiply this average importance value by three. If discharge valve mispositioning is alarmed in the control room or if valve positions are checked regularly (i.e., once per shift, once per day), this failure can be neglected.

20. The accumulators quickly reflood the reactor core following a large LOCA. Each primary loop generally has one accumulator. For successful mitigation of a large LOCA all of the accumulators on the intact loops must inject.

RWST/Containment Sump

21. The containment sump plugging concern can be exacerbated by suction piping design. If a plugged strainer can disable a train of high or low pressure SCCS, multiply the average importance by a factor of 2. Leave importance unchanged if each recirculation train can take suction via multiple sump strainers.

22. Applies only to ice condenser containments.

LPI/RHR High to Low Pressure Interface Design

23. The Westinghouse high to low pressure interface design is the configuration of interest. It features two series check valves with a normally open MOV.

24. The CE design features several check valves in series with a normally closed MOV which is much less susceptible to this initiator. If the check valves are periodically leak tested and the MOV is tested only when the RCS is depressurized, the LPI interfacing LOCA initiator can be neglected.

25. The placement of the accumulator discharge relative to the high/low pressure interface can influence the check valve failure order. For example, Sequoyah's accumulators connect between the two check valves. If the upstream check valve (furthest from the RCS) fails first, the accumulator will discharge into the LPI system and alert the operator. If either interface check valve can fail undetected, this initiator is more likely. Multiply the average importance values by two.

26. Not applicable if the check valves are required to be tested on every RCS repressurization or if the valves change position. Multiply this average importance value by a factor of three if these provisions do not exist.

27. The shutdown cooling (SDC) line initiator appears to be more significant than the LPI interfacing LOCA. The shutdown cooling configuration generally features two normally closed MOVs in series with a relief valve in between. The intervening relief valve makes it necessary that the downstream (furthest from the RCS) fail first. Otherwise, the relief valve discharge would alert the operator and plant shutdown would commence.

28. The shutdown cooling line initiator can be neglected if the MOVs have a high pressure interlock to prevent downstream piping overpressurization and the MOVs are keylocked with administratively controlled keys. Multiply by a factor of three if the pressure interlock is not functional post-startup (Zion).

29. A potential recovery action has been included to account for operator action to isolate the interfacing LOCA by manual closure of the LPI discharge MOV. The successful mitigation of this event is plant specific and is dependent on:

    - The existence of two isolable LPI discharge headers to enable the use of the other LPI loop, or the ability to use another system for RCS makeup.

    - LPI pump separation to minimize the environmental impact of RCS blowdown on the second train.

    - The capability of the LPI discharge MOV to isolate the interfacing LOCA. The valve may not be designed to close against the high differential pressure.

Reactor Coolant Pump Seals

30. Sequence 5 is illustrative of a relative design weakness for certain Westinghouse plants. A single cooling system (CCW) supports reactor coolant pump (RCP) seal cooling modes (thermal barrier cooling and seal injection) and provides essential cooling for the ECCS pumps. The HPI ECCS pumps, i.e., the CVCS charging pumps, provide RCP seal injection and are required to mitigate a RCP seal LOCA failure. However, the pumps are cooled by CCW.

31. The Byron Jackson reactor coolant pumps used in CE plants have a seal configuration (three full pressure seals and a controlled leakoff or a fourth full pressure seal) different from the RCP seals used in Westinghouse plants that provides a greater level of resistance to loss of cooling induced failures.

32. Surry has a cross connect between the units that enables the second unit's charging pumps to supply seal injection to the Unit 1 RCPs in the event of a loss of CCW. This is limited by the Unit 2 RWST capacity and requires makeup from the Unit 1 RWST. Long term mitigation involves RCS depressurization by secondary steaming and LPI/R for injection and long term decay heat removal. At Surry LPI/R operation is not dependent on CCW for either seal or room cooling.

Auxiliary Feedwater System

33. AFW system success criteria vary among the reference plants. Generally, AFW flow from one pump to one steam generator is sufficient for decay heat removal. Sequoyah requires flow to two of its four steam generators and Calvert Cliffs requires operator action to increase AFW flow, if only one steam generator is available.

34. The Calvert Cliffs plant has a pump that is normally locked out and requires manual start. If an AFW pump normally requires operator action to start, increase the average importance value by a factor of four (sequence 6), a factor of 2 (sequence 7) and keep unchanged for sequence 10. If the AFW system has auto start provisions for all pumps, this human error is not applicable.

35. Increase this average importance value by a factor of two if, like Calvert Cliffs, the unavailability of one steam generator requires manual adjustment of the AFW flow control valve to increase flow to the remaining steam generator(s) for successful decay heat removal.

36. If the AFW piping has a common portion of the discharge line, shared by two pumps and selected valves can only be disassembled if both pumps are disabled, multiply by a factor of 3 (sequences 6 and 7). Leave as is for sequence 10.

37. One motor driven AFW pump is usually unavailable as a result of the initiator. Neglect this event if the AFW system has only one motor driven pump.

38. Undetected AFW flow diversion to another unit of a multiple unit site. Based on a single MOV or multiple valves in parallel that isolate an AFW crosstie and the failure of valve position indication. If candidate plant geometry is similar, multiply importance by a factor of 3.

39. The Surry design originally consisted of normally open AFW pump discharge MOVs, insulated discharge lines and check valves that failed to prevent back leakage. After a steam binding incident occurred, check valves were reworked, insulation removed and pump discharge piping temperature was checked every 8 hours. Multiply by a factor of 3 if the design resembles Surry and no compensating measures have been taken.

40. Calvert Cliffs has a common suction header from the CST. For configurations similar to Calvert Cliffs, multiply by a factor of 3.

41. The Sequoyah AFW discharge line configuration utilizes normally open air operated valves that fail closed on loss of air.

Bleed and Feed

42. The availability of bleed and feed is plant specific. Some plant PRAs do not take credit for this option due to the comparatively low head of the safety injection pumps (Calvert Cliffs, NUREG/CR-3511). Other PRAs assume 2 PORVs are required for success (Sequoyah and Surry, NUREG/CR-4550). For those plants with DC controlled PORVs, the sequence 6 initiator (loss of one 125V DC bus), fails one valve and eliminates the bleed and feed mode (Sequoyah). The Surry PORVs use AC control power (with DC backup) and do not have this dependency. The Zion risk assessment (NUREG/CR-4550) has re-evaluated the plant's bleed and feed capability and concluded that a single PORV is sufficient for success.

43. If the bleed and feed success criterion is one out of two PORVs (or if one PORV is not disabled by the initiator), then the PORV operability and human error importances developed from the Zion input (i.e., 23 and 2, respectively) can be used for sequences 6 and 10.

44. If the bleed and feed success criterion requires two PORVs, multiply importance by a factor of 3.

45. The importance value assumes a block valve is closed 20 to 30% of the time. If plant specific experience is higher, this sequence becomes more important, and the reasons for the higher incidence of potential PORV unavailability should be examined.

Emergency Power

46. Some multi-unit sites can supply emergency AC power from one unit to the other. If the Unit 2 EDGs can be readily used to power Unit 1 vital equipment, multiply this importance by a factor of two (sequence 8). This provision is the basis of the average importance estimate for sequence 9 and need not be modified.

47. An inverter fault fails auto actuation of the AFW motor driven pump, and an AFW turbine steam admission valve. One feedwater regulating valve fails closed, and one MFW bypass valve fails full open. An MFW pump minimum flow recirculation valve fails full open and a turbine bypass valve fails closed. These failures are expected to trip the MFW pumps on low suction pressure if the unit of this sequence is at power.

48. Sequoyah has two dedicated EDGs per unit. One EDG is sufficient to prevent an SBO. In addition, a 6.9 kV shutdown can be used to provide AC power from the Unit 2 EDGs.

49. The emergency AC power configuration consists of one dedicated emergency diesel generator (EDG) and one shared EDG for a two unit site. The success criteria is two out of three EDGs to prevent an SBO at either unit. In addition, manual realignment of the swing diesel may be required for a LOOP when the dedicated EDG fails.

50. Zion has two dedicated EDGs per unit and a fifth swing diesel. A single EDG at each unit provides sufficient power to mitigate this sequence.

51. DC power is important to maintain vital instrumentation and as a support system for the turbine driven AFW train(s).

52. The Sequoyah DC power configuration consists of four independent trains with multiple hard wired cross feeds. A fifth battery can be connected to any bus in about ten minutes. In addition, the DC power for the Unit 1 AFW system is normally supplied by the Unit 2 DC buses which are likely to remain operable unless there is a simultaneous SBO at both units.

53. The DC power buses appear to be completely independent between the two Surry units. There does not appear to be a simple mechanism to allow the dedicated EDG at Unit 2 to charge a Unit 1 DC bus.

54. Calvert Cliffs has a DC power design that enables the dedicated Unit 2 EDG to charge two of the four shared DC buses without operator action.

55. Generally, the emergency boration success criteria are one of three charging pumps injecting boron into the RCS with an operable BIT tank or one out of two boric acid transfer pumps supplying sufficient boron to the charging pump suction header. Manual initiation is assumed.

56. The Calvert Cliffs emergency boration success criteria require two charging pumps for boron injection. Most plants require only one pump which is normally running. If multiple charging pumps are required for successful emergency boration, multiply the importance value by a factor of three. If a single pump will suffice, neglect this failure mode.

Emergency Boration

57. The Surry boric acid transfer (BAT) configuration consists of two 100% capacity pumps. Under ATWS conditions, the operator switches the operating BAT pump to its high speed setting. The failure mode is the inability of the operating pump to provide sufficient boron. Since the standby pump must be manually aligned, this recovery was not credited. Multiply importance value by three if the emergency boration configuration resembles Surry.

58. This failure is not applicable for plants that have BIT tanks.

59. Unlike most systems that have multiple injection pathways, Calvert Cliffs has a single normally closed MOV that can fail all boration. Surry has a similar configuration. However, successful emergency boration can also be accomplished through the normal charging path.

Service Water, Component Cooling Water, Room Cooling

60. ECCS injection is usually dependent on the Service Water (SW) and Closed Cooling Water (CCW) systems for cooling. In general, CCW/SW is necessary for high and low pressure ECCS pump seal and lube oil cooling in both the injection and recirculation phases. In addition, room cooling (by SW) is generally required for the recirculation mode.

61. This assessment is based on a CCW success criteria of one out of 3 pumps and one out of two heat exchangers per unit. If the cooling system that supports the ECCS is less redundant, revise the importance value to a 2 (sequence 1) or multiply by a factor of 2 (sequence 5).

62. Calvert Cliffs has a pinch point in the SW system serving the CCW heat exchangers. The closure of an open manual valve in this common line will disable all SW flow to the CCW heat exchangers and ultimately fail. For similar designs, multiply the average importance by a factor of 6.

63. The CCW system is shared between units and is functional during an SBO at one unit. However, the thermal barrier booster heat exchanger pumps are powered by the Unit 1 EDGs, which are unavailable. Therefore, an SBO fails RCP cooling.

64. CCW system is a shared system, and is operable during an SBO at one unit. RCP seal cooling is maintained.

65. This is based on a monthly surveillance. If pump room cooling is tested at six month intervals, multiply by a factor of 6.

6. REFERENCES

1. U.S. NRC Letter (Samuel J. Collins) to Omaha Public Power District (Kenneth J. Morris), January 30, 1990, transmitting the Fort Calhoun Inspection Report, 50-285/89-40.

2. U.S. NRC Inspection Manual, Chapter 2515, Procedure No. 93804, "Risk-Based Operational Safety and Performance Assessment," Revision 0, November 25, 1988.

3. Hester, O.V., et al., "Annotated Bibliography of Reliability and Risk Data Sources," U.S. NRC Report NUREG/CR-5050, March 1988.

4. Bertucio, R.C., et al., "Analysis of Core Damage Frequency from Internal Events: Surry, Unit 1," U.S. NRC Report NUREG/CR-4550, Vol. 3, November 1986.

5. "Millstone Unit 3 Probabilistic Safety Study," Northeast Utilities, August 1983.

6. Garcia, A.A., et al., "A Review of the Millstone 3 Probabilistic Safety Study," U.S. NRC Report NUREG/CR-4142, April 1986.

7. Minarick, J.W., et al., "Precursors to Potential Severe Core Damage Accidents: 1968-1979, A Status Report," U.S. NRC Report NUREG/CR-2497, June 1982.

8. Austin, P.N., et al., "Precursors to Potential Severe Core Damage Accidents: 1980-1981, A Status Report," U.S. NRC Report NUREG/CR-3591, February 1984.

9. Minarick, J.W., et al., "Precursors to Potential Severe Core Damage Accidents: 1985, A Status Report," U.S. NRC Report NUREG/CR-4674, Vols. 1 & 2, December 1986.

10. Minarick, J.W., et al., "Precursors to Potential Severe Core Damage Accidents: 1984, A Status Report," U.S. NRC Report NUREG/CR-4674, Vols. 3 & 4, May 1987.

11. Payne, A.C., et al., "Interim Reliability Evaluation Program: Analysis of the Calvert Cliffs Unit 1 Nuclear Power Plant," U.S. NRC Report, NUREG/CR-3511, March 1984.

12. Bertucio, R.C., et al., "Analysis of Core Damage Frequency from Internal Events: Sequoyah Unit 1," U.S. NRC Report NUREG/CR-4550, Vol. 5, February 1987.

13. Wheeler, T.A., "Analysis of Core Damage Frequency from Internal Events: Zion Unit 1," U.S. NRC Report NUREG/CR-4550, Vol. 7, October 1986.

14. Tullock, W.W., et al., "System Analysis and Risk Assessment System (SARA) Users Manual (Draft, Version 3.0)," U.S. NRC Report NUREG/CR-5022, September 1987.

APPENDIX A

PWR INSPECTION MATRIX DEVELOPMENT

Unlike the accident sequence focus presented earlier, the inspection matrix approach has a system and component emphasis, which is generally more compatible with the bulk of the NRC inspections. The primary purpose of the matrix is to help prioritize and reorganize the inspection items into a user friendly format. PRA insights are included where available, but the inspector should also develop individual avenues of inquiry, on the basis of plant history and his/her own expe[illegible].

Table A-1 is derived from the representative accident sequences. Each "bas[illegible]nt" (i.e., component failure or human error) is listed including originating sequence(s), an impor[illegible]ce estimate for ranking purposes and an inspection matrix that provides recomme[illegible]ded areas of inspection derived from PRA insights and NRC inspection modules.

As discussed in detail in Section 5, for each event, the "importance estimate" is generally the summation of the average importance estimates for all contributing sequences. This value is usually provided, unless the event importance is sensitive to plant specific design or operating variations. In that case, the average importance value is shown in parenthesis and the "comments" provide the necessary guidance to revise the event importance for each contributing sequence as follows:

$$I^{A} = \sum^{R} (I^{A}(R) \cdot P(R))$$

where

I = basic event importance estimate

R = representative accident sequence number

I^{A} = average importance estimate for an event "A" of a representative accident sequence

P = adjustment factor to revise the average importance estimate to incorporate risk significant plant specific design and operating features. This adjustment factor is the same as the Plant Specific Modifiers which accompany Table 5.1.

After the plant specific importance values have been developed, system importances (and rankings) can be determined by summing the appropriate basic event importances in a similar fashion to Table 5.1.

Table A.1

Inspection Items by System

Event Description	Rep. Sequence	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib.	Lic. Oper. Training/ EOPs	
INITIATORS									
LOCAs									
Small/Medium LOCA	1		×		×	×		×	
Medium/Large LOCA	2, 3		×			×		×	
LOCA Outside Containment	4		×	×		×		×	
TRANSIENTS									
Loss of a 125V DC bus	6		×	×	×			×	
Loss of offsite power	7, 8, 9		×	×	×			×	
Loss of the power conversion system	10		×		×		×	×	
A transient that challenges the PPS system	11		×					×	
Loss of all CCW:	5								
• due to a pipe rupture						×		×	
• common cause failure of all CCW pumps				×	×	×		×	
AUXILIARY FEEDWATER SYSTEM									
• Human Error									
Undetected flow diversion	7	(4)	×					×	See note 38, Table 5.1 for potential plant specific modifier application

Notes: 1. See general notes 1, 2 and 3 in the Plant Specific Modifier section accompanying Table 5.1.

2. Importance estimates in parentheses are those which are sensitive to plant design variations, and so have a reference to a PSM in the Comments column.

Table A.1

Inspection Items by System (Cont'd)

Event Description	Rep. Sequence	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib.	Lic. Oper. Training/ EOPs	
AUXILIARY FEEDWATER SYSTEM (Cont'd)									
Failure to restore turbine driven pump from test	6	<1	×	×				×	
Failure to increase flow to SG given unavailability of the other SG	6	(1)	×					×	See note 35, Table 5.1
Operator fails to start locked out pump	6 (7) 10	(7) (12) (9)	×					×	See note 34, Table 5.1
Operator fails to manually start pump, given auto start failure	6, 7	3	×						
Failure to crossfeed AFW from another unit of a multiple unit site	6	3	×					×	
Failure to restore AFW turbine driven pump discharge valve after test	6, 10	<1	×					×	
Failure to manually open turbine driven pump discharge AOVs	8	(1)	×					×	See note 41, Table 5.1
Failure to manually start motor driven pump, given auto start failure	10	(17)	×					×	See note 47, Table 5.1

Notes: 1. See general notes 1, 2 and 3 in the Plant Specific Modifier section accompanying Table 5.1.
2. Importance estimates in parentheses are those which are sensitive to plant design variations, and so have a reference to a PSM in the Comments column.

Table A.1

Inspection Items by System (Cont'd)

Event Description	Rep. Sequence	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib.	Lic. Oper. Training/ EOPs	
AUXILIARY FEEDWATER SYSTEM (Cont'd)									
• Hardware									
Valves									
Throttle/trip valve fails to open (or other valve faults in steam admission line)	6, 7, 10	11		×	×	×	×		
Local fault of valve in MD pump discharge to SG	6	(12)		×	×	×	×		See note 37, Table 5.1
	7	(2)							
Local fault of suction valve from the condensate storage tank fails all operating pumps	7	(2)		×	×	×			See note 40, Table 5.1
	10	(5)							
Local fault of valve in TD pump discharge to SG	6, 7, 8	3		×	×	×	×		
Local fault of valve in MD pump discharge to SG	7	<1		×	×	×	×		
Undetected FW back leakage through pump discharge valves	7	(3)	×	×	×	×			See note 39, Table 5.1
AFW FW valve in maintenance disables two AFW pumps	6	(1)			×				See note 36, Table 5.1
	7	(5)							
	10	(1)							
Maintenance of steam admission valve	10	<1			×				

Notes: 1. See general notes 1, 2 and 3 in the Plant Specific Modifier section accompanying Table 5.1.
2. Importance estimates in parentheses are those which are sensitive to plant design variations, and so have a reference to a PSM in the Comments column.

Table A.1

Inspection Items by System (Cont'd)

Event Description	Rep. Sequence	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib.	Lic. Oper. Training/ EOPs	
AUXILIARY FEEDWATER SYSTEM (Cont'd)									
Pumps									
Motor driven (MD) pump fails to start/run	6 7 10	(16) (2) (2)		×	×	×	×		See note 37, Table 5.1
Turbine driven (TD) pump fails to start/run	6, 7, 8, 10	7		×	×	×	×		
Local fault of MD power breaker	7, 10	2		×	×				
Turbine driven pump in maintenance	6, 7, 10	12			×				
TD pump in test	6, 10	1		×					
Motor driven pump in maintenance	10	<1			×				
AFW Logic									
Local fault of AFW actuation signal logic fails to actuate MD pump and/or TD pump steam valves	10	1		×	×		×		

Notes: 1. See general notes 1, 2 and 3 in the Plant Specific Modifier section accompanying Table 5.1.
2. Importance estimates in parentheses are those which are sensitive to plant design variations, and so have a reference to a PSM in the Comments column.

Table A.1

Inspection Items by System (Cont'd)

Event Description	Rep. Sequence	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib.	Lic. Oper. Training/ EOPs	
EMERGENCY AC POWER SYSTEM									
• Human Error									
Failure to recover AC power	8 9	(25) (27)	×					×	See note 46, Table 5.1
EDG not returned to service from test	7	<1	×	×				×	
• Hardware									
EDG fails to start on demand (incl. common cause)	7, 8, 9	60		×	×		×	×	
EDG fails to continue to run (incl. common cause)	7, 8, 9	31	×	×	×			×	
EDG unavailable due to testing	8, 9	6		×					
EDG unavailable due to maintenance	7, 8, 9	13			×				
HIGH PRESSURE INJECTION/RECIRCULATION SYSTEM									
• Human Error									
Failure to switch from RWST to the containment sump via the LPR system including failure to stop the pumps on RWST low-low alarm	1	(8)	×					×	See note 8, Table 5.1

Notes: 1. See general notes 1, 2 and 3 in the Plant Specific Modifier section accompanying Table 5.1.
2. Importance estimates in parentheses are those which are sensitive to plant design variations, and so have a reference to a PSM in the Comments column.

Table A.1

Inspection Items by System (Cont'd)

Event Description	Rep. Sequence	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib.	Lic. Oper. Training/ EOPs	
HIGH PRESSURE INJECTION/RECIRCULATION SYSTEM (Cont'd)									
• Hardware									
Valves									
Failure of pump return line (mini flow) valve to open fails operating pumps	1	4		×	×	×	×		
Failure of HPI discharge valves to open (incl. common cause)	1	(8)		×	×	×	×		See note 9, Table 5.1
Failure of valve to open in the common portion of the HPI suction line from the RWST (including check valves)	1	2		×	×	×	×		
Plugging of manual valve in the common HPI suction line	1	2		×	×				
HPI pump return line (mini flow) valve fails to close. Interlock fails HPR suction valves.	1	<1		×	×	×	×		
Failure of HPR suction valve(s) to open (incl. common cause)	1	5		×	×	×	×		
Pumps									
Local fault of pump(s) (incl. common cause)	1	2		×	×	×	×		

Notes: 1. See general notes 1, 2 and 3 in the Plant Specific Modifier section accompanying Table 5.1.
2. Importance estimates in parentheses are those which are sensitive to plant design variations, and so have a reference to a PSM in the Comments column.

Table A.1

Inspection Items by System (Cont'd)

Event Description	Rep. Sequence	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib.	Lic. Oper. Training/ EOPs	
HIGH PRESSURE INJECTION/RECIRCULATION SYSTEM (Cont'd)									
Failure of control cable to pump	1	<1		×	×				
Failure of pump breaker to close	1	<1		×	×				
Pump in maintenance	1	<1			×				
LOW PRESSURE INJECTION/RECIRCULATION SYSTEM									
• Human Error									
Failure to switch from cold to hot leg LPR	2	3	×					×	
Failure to stop pumps if pump return line (mini flow) valve fails to open or remain open/failure to restart pump for recirculation	1 3	(1) (1)	×					×	See notes 14 and 18, Table 5.1
Failure to isolate interfacing LOCA	4	(16)	×					×	See note 29, Table 5.1
Failure to successfully switch from LPI to LPR including valve alignment errors	2	(20)	×					×	See note 17, Table 5.1
Failure to realign the system after testing	3	(5)	×	×				×	See note 19, Table 5.1

Notes: 1. See general notes 1, 2 and 3 in the Plant Specific Modifier section accompanying Table 5.1.
2. Importance estimates in parentheses are those which are sensitive to plant design variations, and so have a reference to a PSM in the Comments column.

Table A.1

Inspection Items by System (Cont'd)

Event Description	Rep. Sequence	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib.	Lic. Oper. Training/ EOPs	
LOW PRESSURE INJECTION/RECIRCULATION SYSTEM (Cont'd)									
• Hardware									
Valves									
LPI pump return line (mini flow) valve fails to open or remain open including common cause	1 3	(4) (2)		×	×	×	×		See notes 14 and 18, Table 5.1
Failure of LPR suction valve(s) to open	1 2	(4) (7)		×	×	×	×		See note 15, Table 5.1
Failure of LPI suction valve to close (from RWST)	1 2	(1) (7)		×	×	×	×		See note 15, Table 5.1
LP hot leg recirculation discharge valve fails to open	2	1		×	×	×			
Cold leg isolation valve fails to close	2	4		×	×	×			
Pump discharge crossover valve fails to close	2	<1		×	×	×	×		
Pumps									
LPI pump(s) fail to start (incl. common cause)	1 3	(4) (11)		×	×	×	×		See note 15, Table 5.1
LPI pump(s) fail to run (incl. common cause)	1, 3, 2	8		×	×	×			
Containment sump plugging	1	(1)		×	×				See note 21, Table 5.1

Notes: 1. See general notes 1, 2 and 3 in the Plant Specific Modifier section accompanying Table 5.1.
2. Importance estimates in parentheses are those which are sensitive to plant design variations, and so have a reference to a PSM in the Comments column.

Table A.1

Inspection Items by System (Cont'd)

Event Description	Rep. Sequence	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib.	Lic. Oper. Training/ EOPs	
ACCUMULATOR									
Injection failures (including check valve failure to open/MOV plugging)	3	(27)		×	×	×			See note 20, Table 5.1
COMPONENT COOLING WATER (AUXILIARY COOLANT) SYSTEM									See note 60, Table 5.1
• Human Error									
Failure to manually align standby train after failure of operating loop	1	1	×					×	
• Hardware									
Valves									
Local fault of any CCW valve that disables all ECCS pump coolers	1	<1		×	×	×			
Local fault of standby HX bypass valve	1	1		×	×	×			
Local fault of standby HX outlet or inlet valve	1	<1		×	×	×	×		

Notes: 1. See general notes 1, 2 and 3 in the Plant Specific Modifier section accompanying Table 5.1.
2. Importance estimates in parentheses are those which are sensitive to plant design variations, and so have a reference to a PSM in the Comments column.

Table A.1

Inspection Items by System (Cont'd)

Event Description	Rep. Sequence	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib.	Lic. Oper. Training/ EOPs	
COMPONENT COOLING WATER (AUXILIARY COOLANT) SYSTEM (Cont'd)									
Pumps									
CCW pump(s) fail to start or run (incl. common cause)	1 5	(<1) (25)		×	×	×	×		See note 62, Table 5.1
Standby CCW pump in maintenance	5	(<1)			×				See note 12, Table 5.1
SERVICE WATER									See note 60, Table 5.1
• Hardware									
Valves									
Failure of any SW valve that stops SW flow to a CCW HX	1	(1)		×	×	×	×		See note 61, Table 5.1
Pumps									
Common cause failure of the SW pumps that ultimately cool the high pressure ECCS pumps	1	<1		×	×	×	×		
Strainers									
Common cause failure of HPI cooling water strainers (fails lube oil cooling/seal injection)	1	1		×	×				

Notes: 1. See general notes 1, 2 and 3 in the Plant Specific Modifier section accompanying Table 5.1.

2. Importance estimates in parentheses are those which are sensitive to plant design variations, and so have a reference to a PSM in the Comments column.

Table A.1

Inspection Items by System (Cont'd)

Event Description	Rep. Sequence	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib.	Lic. Oper. Training/ EOPs	
ROOM COOLING									
• Hardware									
Electrical failures (power cable/breaker) disable HPR pump room cooling	1	(3)		×	×				See note 65, Table 5.1
Failure of service water system valve disables HPR pump room cooling	1	(1)		×	×	×			See note 65, Table 5.1
REFUELING WATER STORAGE TANK (RWST)									
• Human Error									
Common cause miscalibration of RWST level sensors fails manual or auto realignment of high and/or low pressure ECCS	1, 2	7		×			×		
Operator fails to remove refuel drain plugs after refuel outage	1	(1)	×		×			×	See note 22, Table 5.1
VITAL BUSES/INVERTERS									
Local fault of inverter fails auto actuation of AFW pump	7	1		×	×				
Loss of vital bus fails TD steam admission valve and MD pump	10	17		×	×				

Notes: 1. See general notes 1, 2 and 3 in the Plant Specific Modifier section accompanying Table 5.1.
2. Importance estimates in parentheses are those which are sensitive to plant design variations, and so have a reference to a PSM in the Comments column.

Table A.1

Inspection Items by System (Cont'd)

Event Description	Rep. Sequence	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib.	Lic. Oper. Training/ EOPs	
BLEED AND FEED MODE									See note 42, Table 5.1
Bleed and feed human error	6	(2)	×					×	See note 43, Table 5.1
PORV fails to open	6 7	(23) (6)		×	×	×			See notes 43 and 44, Table 5.1
PORV block valve closed	7	(1)	×		×				See note 45, Table 5.1
SAFEGUARDS ACTUATION SIGNALS									
Failure of AFW automatic initiation logic	6, 10	3		×			×		
EMERGENCY BORATION									
• Human Error									
Failure to perform (initiate) emergency boration	11	23	×					×	
• Hardware									
Valves									
Local fault of one valve results in system failure	11	(3)							
Control circuit fault of one valve disables system				×	×	×			See note 59, Table 5.1
Power cable to one valve fails, disabling system									

Notes: 1. See general notes 1, 2 and 3 in the Plant Specific Modifier section accompanying Table 5.1.
2. Importance estimates in parentheses are those which are sensitive to plant design variations, and so have a reference to a PSM in the Comments column.

Table A.1

Inspection Items by System (Cont'd)

Event Description	Rep. Sequence	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib.	Lic. Oper. Training/ EOPs	
EMERGENCY BORATION (Cont'd)									
Pumps									
Failure of boric acid transfer pump to provide sufficient flow	11	(2)		×	×	×			See notes 57 and 58, Table 5.1
Maintenance of charging pumps	11	(2)			×				See note 56, Table 5.1
REACTOR PROTECTION SYSTEM									
Failure of RPS	11	28	×	×	×		×		
Failure of manual scram	11	17	×	×	×			×	

Notes: 1. See general notes 1, 2 and 3 in the Plant Specific Modifier section accompanying Table 5.1.
2. Importance estimates in parentheses are those which are sensitive to plant design variations, and so have a reference to a PSM in the Comments column.

APPENDIX B

PREPARATION OF A PLANT SPECIFIC INSPECTION PLAN

The focus of the inspection should be determined at the outset of the preparation. The team leader should decide if the inspection should be conducted using an accident sequence basis, a system/component approach or a combination of both. Each has inherent strengths and weaknesses. The accident sequence approach is an in-depth review with a relatively narrow focus that requires extensive preparation, a detailed plant specific knowledge and operationally oriented inspectors that are also familiar with risk-based techniques. However, the accident sequence context can provide operational insights that might otherwise be overlooked. The system/component framework generally provides a broader scope of inspection items and requires less specialized personnel. The PRA input is usually limited to basic event rankings. The inspectors develop their own lines of inquiry using the Chapter 2515 inspection procedures (Ref. 2), their experience, plant/industry history and previous inspection coverage. Findings are primarily related to hardware.

Tables B.1 and 2 summarize the development process of the accident sequence and component oriented approaches, respectively. The accident sequence basis involves a simulation of selected sequences, either in the control room at a simulator or in the plant for remote actions, using an off-duty, licensed crew. The selection of the accident sequences can be based on previous inspection coverage, operational history and/or the plant-specific sequence importance rankings. Within each sequence, the contributing component failures or human actions are ranked based on importance values derived from the contributing PRAs and plant specific input. These basic events are examined within the context of the accident sequence. For example:

- Are human actions proceduralized, timely and effective? Is the operator familiar with the success criteria for the mitigating or recovery functions? For example, is the operator aware of any time limitations for the initiation of bleed and feed? Are there combinations of PORVs and HPSI pumps that will result in successful decay heat removal?

- Is there a reasonable assurance of system/component operability under accident conditions? For example, if the PORVs are not bench tested at rated conditions, the viability of bleed and feed is suspect, and there is a concern that a PORV may not reset (small LOCA initiator).

- Do degraded plant conditions permit access to remotely operated equipment? Are recovery actions feasible?

Sections 4 and 5 provide detailed guidance, including plant specific accident sequence rankings (for inspection scoping purposes), accident sequence descriptions (for the development of the simulations), and basic event importance values (for inspection prioritization).

The system/component focus is the more traditional inspection approach. As before, the inspection scope can be based on plant operating history, previous inspection coverage and/or PRA-based system or component rankings. Although the representative accident sequences can be reviewed and prioritized for background, the risk-based information is primarily used as a screening tool to rank the inspection items. The inspection plan is generally less prescriptive and defers, to a large extent, to the inspection expertise of the team.

Appendix A provides the necessary information to develop plant specific system/component based inspection guidance for Westinghouse or Combustion Engineering PWRs. Table A.1 is an inspection matrix that combines the failures of the eleven representative sequences. Guidance is provided for the development of plant specific importance estimates for plant features that are risk sensitive. Recommended areas of inspection are also included, derived from the PRA failure modes and the Chapter 2515 inspection procedures.

The accident sequence and component oriented approaches can also be combined. The hybrid inspection combines the accident sequence and component oriented approaches. As illustrated by the Fort Calhoun Station inspection (Section 2.2), selected accident sequences are simulated in conjunction with a component oriented inspection and provide a balance between the narrow focus sequence oriented approach, and the broad, less PRA-intensive, component-based inspection.

The findings and observations developed during the course of a PRA-based inspection should be referenced to the existing body of NRC regulations, if possible. This should be straightforward for the system/component approach, but may be less so for an accident sequence oriented inspection.

The importance of a particular NRC concern may not be obvious to the licensee and should be put in context. The utility management should be provided with the necessary background information to allow them to assess the relevance of the finding to their plant. This is especially important if the utility does not have any in-house PRA expertise.

Table B.1
The Formulation of an Accident Sequence Based Inspection Plan

1. Develop Plant Specific Ranking of the Representative Accident Sequences

   - Use Appendix A (Table A.1) and plant specific design and operating information
   - If no information is available, leave sequence ranking as highly important
   - Cull inappropriate sequences
   - Include additional plant features that can prevent or mitigate the sequence

2. Formulate Inspection Scope

   - Choose the accident sequences of interest based on:
     - plant specific importance ranking
     - previous plant/industry experience
     - previous inspection coverage and findings

3. Develop Plant Specific Basic Event (Component Failure/Human Error) Rankings

   - Use Appendix A (Table A.1) and detailed plant specific information

4. Develop Simulations for the Selected Sequences

   - Use the accident sequence descriptions of Appendix A and plant specific design/operating information
   - Emphasize the risk important events of step 3, above
   - Examine events in the context of the accident sequence

     - human actions - timely?
       - proceduralized?
       - effective?

     - component availability-reasonable assurance of success*

---

* For example, 1) can an MOV be closed under interfacing system LOCA conditions, or 2) is there adequate DC voltage for MOV operation under station blackout conditions?

Table B.2
The Formulation of an Event Based Inspection Plan
(Component Failures and Human Errors)

1. Develop Plant Specific Ranking of Systems, Components and Human Errors

   - Use Appendix A (Table A.1) and plant specific design/operating information
   - If no plant specific information is available, use the average importance value, as listed
   - Cull inappropriate systems, components and human errors

2. Formulate Inspection Scope

   - Select important systems or basic events (i.e., pumps, valves, human errors)
   - Plant specific system or basic event importance rankings
   - Previous plant/industry experience (including precursor studies and NPRDS)
   - Previous inspection coverage and findings

3. Use Basic Event Importance to Prioritize Inspection Items

   - Inspection matrix (Table A.1) provides ranking and general areas for inspection
   - Detailed inspection activities primarily based on the inspector's experience, plant history, nuclear industry events and generic NRC concerns

Table B.3
Sources of Plant Specific Design and Operating Information[1]

P&ID drawings
System Description or training manuals
Technical specifications
FSAR sections

Operations procedures (normal, abnormal and emergency)
Maintenance/surveillance procedures

Records of system modifications
Records of system maintenance

[1] The systems and/or procedures of interest are dependent on the inspection basis (accident sequence or component) as well as the proposed scope.

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, If any.)
NUREG/CR-5637
BNL-NUREG-52260

2. TITLE AND SUBTITLE
Generic Risk Insights for Westinghouse and Combustion Engineering Pressurized Water Reactors

3. DATE REPORT PUBLISHED
MONTH: November YEAR: 1990

4. FIN OR GRANT NUMBER
A-3874

5. AUTHOR(S)
R. Travis, J. Taylor, and A. Fresco, BNL
J. Chung, U.S. NRC

6. TYPE OF REPORT
Formal

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 Radiation Protection and Emergency Preparedness
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

A methodology has been developed to extract generic risk-based information from probabilistic risk assessments (PRAs) of Westinghouse and Combustion Engineering (CE) pressurized water reactors (PWRs) and apply the insights gained to Westinghouse and CE plants that have not been subjected to a PRA. The available PRAs (five Westinghouse plants and one CE plant) were examined to identify the most probable, i.e., dominant accident sequences at each plant. The goal was to include all sequences which represented at least 80% of core damage frequency. If the same plant specific dominant accident sequence appeared within this boundary in at least two plant PRAs, the sequence was considered to be a representative sequence. Eleven sequences met this definition. From these sequences, the most important component failures and human errors that contributed to each sequence have been prioritized. Guidance is provided to prioritize the representative sequences and modify selected basic events that have been shown to be sensitive to the plant specific design or operating variations of the contributing PRAs. This risk-based guidance can be used for utility and NRC activities including operator training, maintenance, design review, and inspections.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)
PWR Type Reactors -- Failures; Reactor - Maintenance; Reactor Components -- failures; human factors -- Risk Assessment; Probabilistic Estimation; failures -- probabilistic estimation loss of coolant -- probabilistic estimation inspection

13. AVAILABILITY STATEMENT
Unlimited

14. SECURITY CLASSIFICATION
(This Page)
Unclassified
(This Report)
Unclassified

15. NUMBER OF PAGES

16. PRICE

THIS DOCUMENT WAS PRINTED USING RECYCLED PAPER.

PRESSURIZED WATER REACTORS