

---

---

# Generic Risk Insights for General Electric Boiling Water Reactors

---

---

Manuscript Completed: February 1991  
Date Published: May 1991

Prepared by  
R. Travis, J. Taylor, 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

**MASTER**

*ds*  
DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

## **DISCLAIMER**

**This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.**

## **DISCLAIMER**

**Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.**

## ABSTRACT

A methodology has been developed to extract generic risk-based information from probabilistic risk assessments (PRAs) of General Electric boiling water reactors and apply the insights gained to plants that have not been subjected to a PRA. The available risk assessments (six plants) 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. Eight 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.

## CONTENTS

	<u>Page</u>
ABSTRACT . . . . .	iii
LIST OF TABLES . . . . .	vii
EXECUTIVE SUMMARY . . . . .	viii
ACKNOWLEDGEMENTS . . . . .	xi
NOMENCLATURE . . . . .	xii
1. INTRODUCTION . . . . .	1-1
1.1 Objective . . . . .	1-1
1.2 Background . . . . .	1-1
1.3 Scope and Limitations . . . . .	1-1
1.4 Report Structure and Logic . . . . .	1-2
2. POTENTIAL APPLICATIONS OF THE METHODOLOGY . . . . .	2-1
2.1 Applications to Plant Operations . . . . .	2-1
2.2 Trial Application of the Methodology . . . . .	2-2
2.3 Major Risk Significant Insights . . . . .	2-4
3. DEVELOPMENT OF REPRESENTATIVE ACCIDENT SEQUENCES FOR GE BWRs. . . . .	3-1
3.1 Establishment of the PRA Data Base . . . . .	3-1
3.2 The Representative BWR Accident Sequences . . . . .	3-1
4. PLANT SPECIFIC DESIGN AND OPERATING INSIGHTS . . . . .	4-1
4.1 Representative Accident Sequence 1: Loss of High Pressure Injection and Failure to Depressurize . . . . .	4-1
4.2 Representative Accident Sequence 2: Loss of Containment Heat Removal . . . . .	4-3
4.3 Representative Accident Sequence 3: Station Blackout with Intermediate Term Failure of High Pressure Injection . . . . .	4-5
4.4 Representative Accident Sequence 4: Station Blackout with Short Term Failure of High Pressure Injection . . . . .	4-7
4.5 Representative Accident Sequence 5: ATWS with Failure of RPV Water Level Control at High Pressure . . . . .	4-8
4.6 Representative Accident Sequence 6: ATWS with Failure of RPV Water Level Control at Low Pressure . . . . .	4-9
4.7 Representative Accident Sequence 7: ATWS with Failure of Standby Liquid Control (SLC) Injection . . . . .	4-11
4.8 Representative Accident Sequence 8: Unisolated LOCA Outside Containment . . . . .	4-12

**CONTENTS (cont'd)**

	<u>Page</u>
5. IDENTIFICATION OF RISK IMPORTANT SYSTEMS, COMPONENTS, AND HUMAN ACTIONS .....	5-1
5.1 Calculation of Average System and Event Importances .....	5-2
5.2 Development of Plant Specific Modifiers .....	5-4
5.3 Ranking of the Basic Events .....	5-5
6. REFERENCES .....	6-1
APPENDIX A - BWR INSPECTION MATRIX DEVELOPMENT .....	A-1
APPENDIX B - PREPARATION OF A PLANT SPECIFIC INSPECTION PLAN ...	B-1

## LIST OF TABLES

<u>No.</u>		<u>Page</u>
3.1	PRA Data Base Used to Develop the BWR Representative Accident Sequence List	3-2
3.2	Plant Specific Dominant Accident Sequence Criteria .....	3-3
3.3	Representative BWR Accident Sequences .....	3-4
3.4	Plant Specific Core Damage Distribution .....	3-5
4.1	Representative Sequence Prioritization Summary .....	4-14
5.1	Representative Accident Sequence Importance Summary .....	5-6

## 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 boiling water reactors (BWRs) with General Electric (GE) nuclear steam supply systems (NSSS). 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 GE 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.

At the time when this methodology was formulated, six PRAs for GE plants, were available in a format suitable for evaluation.

The NRC has mandated that nuclear power plant licensees develop individual plant evaluations (IPEs) via Generic Letter 88-20. Most of the licensees are expected to 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 potentially 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 that are considered to be representative of the most risk-significant accident sequences of GE BWRs. These accident sequences can be summarized as follows:

- Transient sequences
- Station blackout (SBO) sequences
- Anticipated transient without scram (ATWS) sequences
- Loss of coolant accident (LOCA) outside containment sequence

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. Eight accident sequences met this definition.

The core damage frequency distribution among the representative sequences shows marked differences from plant to plant. Such differences are partially attributable to the design and operational variations. The 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. The information or insights gained from this study 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 to specific systems. For events which are sensitive to variations in plant design or operating conditions, appropriate plant specific modifying factors are provided. This allows estimation of the plant specific relative importance of components and systems.

The inspection matrix itself provides guidance in the following areas:

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

#### Risk-Significant, Plant Specific Design Factors

Boiling Water Reactors typically incorporate many diverse systems for inventory makeup and decay heat removal. In general, this diversity makes BWRs less vulnerable to random failures in comparison to pressurized water reactors. Consequently, common mode failures become more dominant, even for support systems. The PRA modeling of common mode failures have a higher degree of uncertainty than other types of failures due to their relatively low occurrence rates. This uncertainty has resulted in modeling differences among the contributing PRAs which can have a substantial influence on the plant specific contribution to a representative accident sequence. Where applicable, these assumptions are addressed within the appropriate sequences and considered in the qualitative assessment of sequence importance. The foregoing discussion notwithstanding, this study has identified risk significant, plant specific design factors which can have a significant influence on relative importance of the sequences, systems or components. These design factors are summarized below.

- The feedwater (FW) system is the normal source of high pressure reactor pressure vessel (RPV) makeup. Unlike a turbine driven system, motor driven feedwater pumps are not disabled by MSIV closure. Plants with motor driven feedwater pumps have a highly reliable, normally operating source of high pressure injection that is unaffected by the majority of the initiators that comprise the general transient category.
- Older BWRs that have Feedwater Coolant Injection Systems and Isolation Condensers have limited decay heat removal diversity at high reactor pressure. The initiators that disable feedwater, such as a loss of off-site power, are considerably more important for these plants.
- An Automatic Depressurization System (ADS) initiation logic that requires coincident high drywell pressure and low reactor pressure vessel (RPV) level may not automatically initiate during a transient initiated sequence. This loss of an automatic backup to the proceduralized manual depressurization requirements, reduces the overall success probability of the depressurization function.

- The ADS inhibit switch is an important ATWS mitigation feature that eliminates the periodic resetting of the ADS timer and reduces the likelihood of uncontrolled vessel blowdown.
- The general transient initiator is dominated by the more frequent occurrences, such as turbine trip and MSIV closure. The loss of off-site power (LOOP) accounts for approximately 2% of the initiator. Given the availability of off-site power, the motor driven high pressure core spray (HPCS) is more reliable than its turbine driven counterpart.
- The degree of redundancy in the emergency AC (EAC) power system is influential in reducing the probability of the Station Blackout scenarios. Multi-unit sites frequently have hardwired administratively controlled bus crossties that can provide significant flexibility. This assessment of EAC redundancy must also consider support system failures. Emergency Diesel Generators (EDGs) that use the same DC bus or Service Water Train are not totally independent.
- The service water system provides EDG jacket water cooling. The system diversity determines its contribution to Station Blackout. A design that allows multiple trains to provide diesel cooling is less vulnerable to SW induced EDG failures, as compared with a strictly divisional configuration.
- The standby liquid control (SLC) compliance alternative that was adopted to meet the 86 gpm equivalent injection requirement of 10CFR50.62 influences system reliability, and the relative importance of the human error and hardware contributions. The enriched boron option preserves the system redundancy which reduces the importance of individual component failures. The relatively low contribution of system hardware failures results in a higher proportion of system failures due to human error. The two pump alternative requires the simultaneous operation of both SLC trains. Given an 86 gpm injection requirement, this alternative is more vulnerable to hardware failures. Thus, the same human error probability tends to have a lower percentage contribution to the overall system failure estimate.

## **ACKNOWLEDGEMENTS**

The authors wish to thank William D. Beckner and Steven Long of the NRC for their insightful guidance in preparing this document. Our grateful appreciation is also extended to John Boccio, Adele DiBiasio and Anthony Fresco of BNL for their expert comments and advice. Donald Caphton, Theodore Easlick, M. Wayne Hodges and Carl Sisco of the NRC, Region I, were instrumental in the field applications of this methodology. Finally, Ann Fort typed this document, corrected our grammatical lapses and is responsible for the polished report you are about to read.

## NOMENCLATURE

AC	Alternating Current
ADS	Automatic Depressurization System
ATWS	Anticipated Transient Without Scram
BWR	Boiling Water Reactor
BWROG	BWR Owner's Group
CCW	Component Cooling Water
CDF	Core Damage Frequency
CRD	Control Rod Drive
CRDH	Control Rod Drive Hydraulic
CS	Core Spray
DC	Direct Current
DG	Diesel Generator
EAC	Emergency Alternating Current
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EOP	Emergency Operating Procedure
EPG	Emergency Procedure Guideline
FW	Feedwater
FWCI	Feedwater Coolant Injection
GE	General Electric Company
HCTL	Heat Capacity Temperature Limit
HEP	Human Error Probability
HPCI	High Pressure Coolant Injection
HPCS	High Pressure Core Spray
HPI	High Pressure Injection
HVAC	Heating Ventilation and Air Conditioning
HX	Heat Exchanger
IC	Isolation Condenser
ICMUP	Isolation Condenser Makeup
IPE	Individual Plant Evaluation
IREP	Interim Reliability Evaluation Program
ISI	In-Service Inspection
ISLOCA	Interfacing Systems LOCA
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LPI	Low Pressure Injection
LPCI	Low Pressure Coolant Injection
MDP	Motor Driven Pump
MOV	Motor Operated Valve
MSIV	Main Steam Isolation Valve
NRC	U.S. Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
PCS	Power Conversion System
PSM	Plant Specific Modifier
PRA	Probabilistic Risk Assessment
PSS	Probabilistic Safety Study

## NOMENCLATURE (Cont'd.)

RBCCW	Reactor Building Closed Cooling Water
RCIC	Reactor Core Isolation Cooling
RCS	Reactor Coolant System
RHR	Residual Heat Removal
ROSPA	Risk-Based Operational Safety and Performance Assessment
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RWCU	Reactor Water Cleanup
SBO	Station Blackout
SDC	Shutdown Cooling
SLC	Standby Liquid Control
SORV	Stuck Open Relief Valve
SRVs	Safety Relief Valves
SSES	Susquehanna Steam Electric Station
STI	Surveillance Test Interval
SW	Service Water
T&M	Test and Maintenance
TAF	Top of Active Fuel
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 application to GE BWRs that do not have 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 (internal events) of the plant specific PRAs from which they were derived<sup>1</sup>.

### 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 GE 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 the 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 is developed on the basis of functional aspects of plant systems and 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 generally not addressed<sup>2</sup> 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. This application is focussed on the General Electric BWR designs.

---

<sup>1</sup> For readers not familiar with PRA terminology, a more detailed explanation of the terms used in this report is provided in Section 5, page 5-1.

<sup>2</sup> However, representative accident sequence 2 credits containment venting as a means to prevent core damage due to potential ECCS failures after a containment over-pressurization failure.

Almost by definition, any usable generic application of PRA insights 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 potential applications include prioritization of maintenance activities, evaluation of plant modifications, operator training and plant configuration controls. The results of trial application at the Susquehanna Steam Electric Station and at a Mark I BWR are presented, as well as the major overall insights arising from this effort.

The report then presents the eight representative accident sequences for GE BWRs (Section 3) that were developed from the PRAs of six BWRs (see Table 3.1). The representative accident sequences were 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 for GE BWRs without 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 a generic risk-based inspection matrix which is a composite, ranked listing of the basic events with recommended areas of inspection. Unlike the accident sequence orientation of 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 "system-based" matrix for a particular plant, using Table A.1.

## 2. POTENTIAL APPLICATIONS OF THE METHODOLOGY

Although a plant specific PRA is certainly preferable, the methodology that will be described 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. The details of the application process will become more evident to the reader during the review of this document.

### 2.1 Application 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 plant vulnerability insights beyond single failure criteria, so as to mitigate and/or to recover from the event situations. The objective is to familiarize the operations personnel 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 safety-related components and energy production-related equipment, as well as those added by plant management.

The list may vary from one plant to another, even among the plants with similar design. The plant's critical components can be prioritized on the basis of the relative risk importance for input into 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 the prevention of core damage or to avoid 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. The appropriate application of the reliability concept in conjunction with the risk insights can reduce outages of critical components for maintenance or surveillance, and can provide a basis for good predictive and preventive maintenance programs.



### 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 an 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. The generic insights would be particularly valuable for an evaluation of plant risk with respect to the Individual Plant Evaluation (IPE) process and elements of Generic Letter 88-20.

Another application is the review 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, either regulatory or self-assessment, 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 Susquehanna and a Mark I BWR

The methodology was applied as part of the October 1990 Maintenance Team Inspection at the Susquehanna Steam Electric Station (SSES). The generic information was revised, as appropriate to reflect the SSES design. A risk based ranking of systems and components was developed to assist in the prioritization of the inspection effort.

For example, this information was used to screen Susquehanna LERs, Significant Operating Occurrence Reports and Work Authorizations. Areas that were selected for detailed review of the licensee's root cause analysis program and the work authorization prioritization process included:

- Scram Discharge Volume high water level trip annunciation
- HPCI and RCIC relay coil failures
- RPS relay and breaker concerns
- RWCU containment isolation valve torque switch misadjustment
- MSIV limit switch problem
- CRD nitrogen accumulator and pump corrective maintenance
- ADS instrument nitrogen system degradation

The root cause analysis and the prioritization of corrective maintenance associated with each occurrence was evaluated within the context of the NRC maintenance inspection guidance (Refs. 1 & 2). It should be noted that SSES has a plant specific PRA that is used for risk management. Although

the generically derived system/component prioritization correlated well with the Susquehanna IPE, the list of plant specific dominant accident sequences differs somewhat from the representative accident sequences developed in Section 3. The earlier revisions of the SSES PRA showed a better correlation to the generic methodology. Each PRA revision generated key plant modifications or procedural revisions that addressed the major core damage contributors to risk. As a result "typical" BWR accident sequences do not necessarily dominate the SSES core damage frequency estimate.

For example, in response to a potential common cause loss of HPCI and RCIC due to battery depletion during station blackout (SBO), a portable 100KW diesel generator (DG) was purchased. This DG is dedicated to station battery charging during SBO. As a result, SBO with intermediate failure of high pressure injection (representative accident sequence 3) is no longer a major contributor to the SSES core damage frequency.

This illustrates the impact that design and operating variations can have on the plant specific contribution to the representative accident sequences. Although the available BWR risk significant plant variations are discussed in subsequent sections of this report, the list is, by no means complete. Care should be exercised to ensure that unusual plant features that can affect risk are recognized and incorporated into the qualitative importance assessment for each representative accident sequence.

The methodology was validated in real time during recent simulations at a Mark I BWR. Accident sequences, including key operator errors, were run on the plant simulator. Decision times, operator interaction, the use of the plant specific EOPs and potential sources of human error were evaluated. The following insights on operator and plant performance were observed:

- The operators appear to be very sensitive to ATWS.
- Motor driven feed pumps provide a reliable source of high pressure injection. Unlike their turbine driven counterparts, a feedwater system with motor driven pumps can remain operable after a transient induced MSIV closure.
- A swing diesel that can be aligned to either emergency bus is a significant design feature that could reduce plant vulnerability to SBO sequences.
- A typical PRA accident sequence is the loss of high pressure injection with a failure to depressurize the reactor vessel (representative accident sequence 1). Older PRAs typically had a significant human failure estimate for the manual RPV depressurization, based on unclear or conflicting procedural guidance. The development of plant specific emergency operating procedures (EOPs) based on the BWROG guidelines clearly requires RPV depressurization following a loss of HPI. This is expected to reduce the human error estimate for manual RPV depressurization.
- The BWR EOPs provide clear directions for SLC initiation that is based on torus water temperature<sup>1</sup>. This is a significant improvement over earlier BWR procedures. Although the estimated human error associated with SLC initiation has decreased because of increased procedural clarity, the actual timing may vary. Some operators, by training or inclination, may initiate SLC early in anticipation of the required procedural action. Others may delay until the

---

<sup>1</sup>The boron injection initiation temperature is a plant-specific setpoint. It is 105° at this plant.

suppression pool boron injection initiation temperature is reached. This potential variation can be exacerbated by MSIV closure due to the demands on the operating crew and the rapid rise in torus temperature. (The authors observed one MSIV closure ATWS scenario where SLC was initiated at a torus temperature of 140°F.) Therefore, the uncertainty associated with ATWS events is not limited to SLC initiation times and the PRA modeling must account for these sources of uncertainty.

### 2.3 Major Risk Significant Insights

This study has provided the insights on the operation and design features of BWRs that can potentially have major risk significance. These include:

- The feedwater (FW) system is the normal source of high pressure RPV makeup. Unlike a turbine driven system, motor driven feedwater pumps are not disabled by MSIV closure (i.e., loss of high pressure steam). The majority of the risk-significant transient initiators result in initial or subsequent MSIV closure. Plants with motor driven feedwater pumps have a highly reliable, normally operating source of high pressure injection that is unaffected by the majority of the initiators that comprise the general transient category.
- Older BWRs that have Feedwater Coolant Injection Systems (without other independent high pressure injection systems) and Isolation Condensers have limited decay heat removal diversity at high reactor pressure. The initiators that disable feedwater, such as a loss of offsite power, are considerably more important for these plants.
- An Automatic Depressurization System (ADS) initiation logic that requires coincident high drywell pressure and low reactor pressure vessel (RPV) level may not automatically initiate during a transient initiated sequence. This loss of an automatic backup to the proceduralized manual depressurization requirements, reduces the overall success probability of the depressurization function.
- The ADS inhibit switch is an important ATWS mitigation feature, that eliminates the periodic resetting of the ADS timer and reduces the likelihood of uncontrolled vessel blowdown.
- The general transient initiator is dominated by the more frequent occurrences, such as turbine trip and MSIV closure. The loss of offsite power (LOOP) accounts for approximately 2% of the initiator. Given the availability of offsite power, the motor driven high pressure core spray (HPCS) is more reliable than its turbine driven counterpart.
- The degree of redundancy in the emergency AC (EAC) power system is influential in reducing the probability of the Station Blackout scenarios. Multi-unit sites frequently have hardwired administratively controlled bus crossties that can provide significant flexibility. This assessment of EAC redundancy must also consider support system failures. Emergency Diesel Generators (EDGs) that use the same DC bus or Service Water train are not totally independent.
- The service water system provides EDG jacket water cooling. The system diversity determines its contribution to Station Blackout. A design that allows multiple trains to provide diesel cooling is less vulnerable to SW induced EDG failures, as compared with a strictly divisional configuration.

- The SLC compliance alternative that was adopted to meet the 86 gpm equivalent injection requirement of 10CFR50.62 influences system reliability, and the relative importance of the human error and hardware contributions. The enriched boron option preserves the system redundancy which reduces the importance of individual component failures. With a relatively low system hardware contribution the proportion of system failures due to human error becomes higher. The two pump alternative requires the simultaneous operation of both SLC trains. Given an 86 gpm injection requirement, this alternative is more vulnerable to hardware failures. Thus, the same human error probability tends to have a lower percentage contribution to the overall system failure estimate.

When these insights 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 GENERAL ELECTRIC BWRs WITHOUT PLANT RISK ASSESSMENTS**

This section presents the first phase of the methodology. Risk insights from PRAs of GE BWRs that were available in 1988 were extracted for application to other BWRs not already subjected to a PRA. As explained in Section 1, risk assessments were used as a data base to develop eight BWR representative accident sequences. These sequences form the basis of a generic PRA application that will examine plant specific influences on sequence importance and basic event prioritization, as described later in this report.

#### **3.1 Establishment of the PRA Data Base**

Since dominant accident sequence descriptions are readily available, six plants (see Table 3.1) form the PRA data base that was used to develop the representative accident sequences for this program. Both the IREP study and the utility PRA were included for Millstone, Unit 1.

#### **3.2 The Representative BWR 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 to capture 80% (minimum) of 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.

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 are also important 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, 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 included. Table 3.3 lists the representative BWR accident sequences. Boiling water reactors, as a class, exhibit less NSSS design diversity than PWRs. This results in a smaller number of BWR representative sequences than were developed for PWRs (Ref. 3).

Table 3.4 provides the distribution of core damage frequencies from the six base plants among the representative accident sequences. The distribution is consistent with the risk assessments that were used as the data base as it reflects the range of core damage contributors. Some of these differences can be attributed to both design variations in the support systems and procedural improvements. However, PRA modeling differences are also a significant influence. The Millstone Unit 1 results reflect both of these influences.

Table 3.4 also shows the fraction of core damage frequency that is accounted for by the representative sequences. It 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.

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 BWR Representative Accident Sequence List

Plant	Reactor, Containment Type §	PRA Documents
1. Limerick	BWR4, Mark II	Probabilistic Risk Assessment, Limerick Generating Station, March, 1981, Philadelphia Electric Co.
2. Plant A*	BWR4, Mark II	Utility PRA
3. Millstone, Unit 1	BWR3, Mark I	Millstone Unit 1, Probabilistic Safety Study, July 1985, Northeast Utilities Interim Reliability Evaluation Program, NUREG/CR-3085 +
4. Plant B*	BWR3, Mark I	Utility PRA +
5. Peach Bottom Unit 2	BWR4, Mark I	Analysis of Core Damage Frequency from Internal Events, NUREG/CR-4550, Vol. 4 + System Analysis and Risk Assessment (SARA), Version 3.0 +
6. Grand Gulf	BWR6, Mark III	NUREG/CR-4550, Vol. 6 + SARA, Version 3.0 +

§ General Electric is the NSSS vendor for all plants in the data base.

\* Withheld at the utility's request.

+ Also used to formulate system and basic event importances.

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 <sup>1</sup>	Percent of Core Damage Frequency Addressed by the Methodology
Limerick	10	87	8	79
Plant A	11	80	9	72
Millstone 1 - IREP	10	93	10	93
Millstone 1 - Utility PRA	13	80	13	80
Plant B	10	94	9	92
Peach Bottom 2	10	97	9	96
Grand Gulf	10	99	10	99

3-3

<sup>1</sup> If a sequence appears in two or more plant specific PRA dominant accident sequence listings, it is designated as a representative sequence.

Table 3.3 Representative BWR Accident Sequences +

1. Transient or small LOCA initiator with the loss of high pressure injection and a failure to depressurize.
2. Transient or LOCA initiator followed by the loss of all containment heat removal.
3. Station blackout with failure to recover offsite power resulting in an intermediate term failure of high pressure injection.
4. Station blackout with short term failure of high pressure injection.
5. Transient initiator with initial or subsequent MSIV closure, failure to scram and a failure of RPV water level control at high pressure.
6. Transient initiator with initial or subsequent MSIV closure, failure to scram and a failure of RPV water level control at low pressure.
7. Transient initiator with a failure to scram and a failure of Standby Liquid Control (SLC) injection.
8. LOCA outside containment.\*

---

+ The sequences are described in detail in Section 4.

\* Specified because of potentially serious offsite consequences.



Table 3.4 Plant Specific Core Damage Distribution

Represent. Sequence # (from Table 3.3)	Percent of Core Damage Frequency (CDF)						
	Limerick	Plant A	Millstone 1 IREP	Millstone 1 PRA	Plant B	Peach Bottom	Grand Gulf
1	48	66	50	18	10+	+	-
2	+	3	10	53	3+	-	-
3	27+	+	-	-	36+	29	81
4	+	+	26	9	-	55	17
5	4**	+	**	+	19	4	1
6	**	+	**	+	16+	-	-
7	+	3	7	+	8	8	<1
8	-	+	-	+	+	-	-
Dominant Accident Total*	79	72	93	80	92	96	99

\* 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.

\*\* PRA modeling predated current emergency operating procedure guidance for ATWS events related to RPV level control.

- The PRA does not contribute to this representative accident sequence.

#### 4. PLANT SPECIFIC DESIGN AND OPERATING INSIGHTS

As previously discussed, Table 3.4 provides the core damage frequency (CDF) distribution of the six reference 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 eight 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. Table 4.1 provides a synopsis of this section. A qualitative estimate of sequence importance (high, medium, low) is presented for each representative accident sequence for each of the four reference plants. The sequence importance estimates generally reflect the core damage frequency distributions of Table 3.4. Where a significant disparity exists, the rationale for the qualitative importance estimate is presented in the appropriate sequence discussion of Section 4. Qualitative success estimates for the critical functions or systems that contribute to the sequence are assessed. Within the context of a sequence, if a plant function has no distinguishing features, it is arbitrarily assigned an "average" success estimate for that plant. The same function is examined for the remaining reference plants. Success estimates are assigned (higher, average, lower) relative to the benchmark "average" based upon design or operating variations that are assessed to increase or decrease the likelihood of success. The process continues until all the critical functions that contribute to a representative accident sequence are reviewed.

The Limerick, Plant A and the Millstone 1 Utility PRAs did not provide detailed dominant accident sequence failure modes (cutsets) so no specific system assessments could be made for these PRAs and they do not appear in Table 4.1.

##### 4.1 Representative Accident Sequence 1: Loss of High Pressure Injection and Failure to Depressurize

###### Sequence Description

Representative Sequence 1 is initiated by a general transient<sup>1</sup>, or a small break LOCA. The reactor successfully scrams. Subsequently, the power conversion system (PCS) is lost.

The loss of HPCI (HPCS) and RCIC is caused by hardware failures (primarily pump faults) and system unavailability due to test or maintenance activities. The control rod drive hydraulic (CRDH) system can also be used as a high pressure makeup. Major faults include operator failure to start the second CRDH pump or failure to align flow control station valves to maximize system flow. Feedwater coolant injection (FWCI) system failures are due to pump breaker problems or support system malfunctions.

---

<sup>1</sup> The general transient initiator is composed of the following:

Turbine trip with subsequent MSIV closure	(50%)
MSIV closure and loss of condenser vacuum	(30%)
Loss of main feedwater	(15%)
Inadvertent opening of an SRV with MSIV closure	(3%)
Loss of offsite power	(2%)

Emergency AC power failures such as output breaker or generator hardware faults are important to motor driven HPI sources.

The most important basic events in this sequence involve failure of depressurization, particularly the common cause failure of the SRVs or the failure to manually depressurize the RCS. The failure to depressurize the RPV after HPI failure results in core damage due to a lack of vessel makeup.

#### Plant Specific Design and Operating Insights

As presented in Table 3.4, the plant specific core damage frequency contributions to representative accident sequence 1 range from 66% (Plant A) to far less than 1% (Grand Gulf). The four reference plants (for which accident sequence cutsets were available) were reviewed to assess the impact of plant specific design or operating variations on sequence contribution. The major design features that can influence risk are listed below:

- The feedwater (FW) system is the normal source of high pressure RPV makeup. Unlike a turbine driven system, motor driven feedwater pumps are not disabled by MSIV closure. Plants with motor driven feedwater pumps have a highly reliable, normally operating source of high pressure injection that is unaffected by the loss of high pressure steam and is less vulnerable to the majority of the initiators that comprise the general transient category. In general, plants with motor driven feedpumps are less vulnerable to this sequence and the contribution is largely attributable to those initiators that directly disable feedwater or that affect the power supply to the pump breaker.
- Feedwater coolant injection (FWCI) systems use one FW train for high pressure injection and the plants with FWCI systems generally do not have other independent high pressure injection/decay heat removal systems other than the isolation condenser<sup>2</sup>. Unlike later BWR designs, a loss of offsite power at plants of this type results in a limited HPI and decay heat removal capability, comprised of FWCI and the isolation condenser (IC).<sup>3</sup>
- Millstone uses a gas turbine emergency power source as a support system to both the FWCI and the IC makeup (ICMUP) system<sup>4</sup>. As identified in the IREP, the loss of the gas turbine after a LOOP disables all high pressure injection.
- A stuck open relief valve (SORV) is important because it allows the loss of sufficient RCS inventory to effectively disable the lower capacity high pressure injecting systems, such as the CRDH and possibly, the RCIC system. In addition, an SORV defeats the isolation condenser.

---

<sup>2</sup> Examples include: Oyster Creek, Nine Mile Point 1 and Millstone 1.

<sup>3</sup> Dresden 2 and 3 are exceptions. They also have an independent high pressure injection system.

<sup>4</sup> A normally closed ICMUP valve was the only component that required AC power for long term operation of the isolation condenser. The Millstone 1 IREP credited local recovery of isolation condenser makeup by manually opening this valve. This design vulnerability was subsequently addressed by changing to a DC powered valve.

- The High Pressure Core Spray system generally appears to be more reliable than its turbine driven counterpart. This is especially applicable for sequences initiated by general transients because the majority of the contributing initiators, such as turbine trip, MSIV closure, etc., retain offsite power which is an important consideration for HPCS operation.
- The Millstone and Grand Gulf ADS logic requires coincident high drywell pressure and low RPV level signals for automatic initiation. Within the context of this sequence, a high drywell pressure signal may not occur. If a coincident high drywell pressure signal is not required, ADS can function as a backup to the manual RPV depressurization required by the BWROG EPGs.

The small Peach Bottom and Grand Gulf contributions to this sequence appear to be caused by different modeling assumptions with regard to ADS. GE BWRs can have up to eleven safety relief valves. Two SRVs are generally sufficient for RPV depressurization. Since it is unlikely that ten valves will fail randomly, the common mode failure dominates system unavailability. Common mode failures are relatively rare and their application for PRA purposes, has a high degree of uncertainty. For example, both Plant B and Peach Bottom postulate common mode failures of the ADS valves. Plant B applies this failure to the remaining SRVs also. Peach Bottom assumes that the non ADS SRVs are available for manual depressurization. This assumption reduces the core damage frequency for this sequence by a factor of 100 and is the major reason for the wide variation in plant specific contributions to representative accident sequence 1.

#### Qualitative Estimate of Sequence Importance

The foregoing assessment of plant specific ADS and HPI design and operating variations, in conjunction with the core damage contributions of Table 3.4, indicates that representative accident sequence 1 is generally of medium importance. At Millstone Unit 1 this sequence has a high importance, primarily due to the impact of the LOOP initiator on the high pressure injection function. Table 4.1 presents the importance estimates for all eight representative accident sequences, resulting from the assessed availability of key functions and systems.

#### 4.2 Representative Accident Sequence 2: Loss of Containment Heat Removal

##### Sequence Description

Representative sequence 2 is initiated by a general transient<sup>5</sup>. The reactor successfully scrams and RCS makeup is available. The initial or subsequent closure of the MSIVs isolates the most important decay heat removal mechanism, the power conversion system (PCS).

---

<sup>5</sup> The general transient initiator is composed of the following:

Turbine trip with subsequent MSIV closure	(50%)
MSIV closure and loss of condenser vacuum	(30%)
Loss of main feedwater	(15%)
Inadvertently opened SRV with MSIV closure	(3%)
Loss of offsite power	(2%)

The RHR system is the alternate to PCS for decay heat removal. This sequence postulates failures of key RHR components such as minimum flow, heat exchanger bypass or suppression pool return valves, the plugging of the suppression pool strainers or RHR loop test and maintenance unavailability.

Service Water (SW) system failures are the major cause of RHR system unavailability. Key hardware faults are: service water pump failures and RHR heat exchanger plugging on the service water side. The unavailability of the RHR heat exchanger due to SW test and maintenance is also significant.

Containment isolation and the loss of the RHR system results in decay heat rejection to the suppression pool via the SRVs. The pool heats up, starts to boil and pressurizes the containment. Subsequently, containment venting fails. Note that this is one of the few sequences where containment venting can preclude core damage. The primary containment ultimately fails on overpressure. RPV injection is subsequently assumed to fail (due to the effects of containment failure) resulting in core damage.

#### Plant Specific Design Operating Insights

The plant specific CDF contributions associated with representative accident sequence 2 are small, generally reflecting the long recovery time associated with a loss of decay heat removal sequence. The major design features that can influence sequence importance are the diversity of the decay heat removal systems (and the associated support systems). The decay heat removal function can be influenced by the following design features:

- Millstone Unit 1 has separate LPCI/containment cooling and shutdown cooling systems, with a total of four heat exchangers. The LPCI/containment cooling system uses emergency SW, a standby system for cooling. The SDC system uses RBCCW and normal service water which continually operate. The diversity of these cooling systems makes Millstone less vulnerable to the loss of the decay heat removal function from random equipment failures. Rather, common cause failures are the major contributors to this sequence.
- In general, the previously described separation of the containment cooling and shutdown cooling functions provides greater diversity of the decay heat removal function. In practice this can be limited by support system diversity. For example at Millstone, the shutdown cooling system has single inlet and outlet AC powered MOVs which are each powered by a different bus. Thus a LOOP with the loss of an EAC source disables the remote initiation of shutdown cooling, as well as, one train of containment cooling.
- A major common cause failure at Millstone is the loss of instrument AC power due to breaker or bus transfer malfunctions. This disables the associated train of shutdown cooling and containment cooling. These components are not normally operating and, at the time of the IREP, were not periodically tested. Thus failures would normally be discovered upon system demand.
- The loss of an EAC source, given a LOOP initiator is important at most plants because it disables one train of decay heat removal. Multi-unit sites with shared buses or the availability of bus cross-ties can reduce the significance of the LOOP initiator for this sequence.

## Qualitative Estimate of Sequence Importance

As stated above, the assessed availability of the decay heat removal function and the supporting systems determines the importance of this sequence. Representative accident sequence 2 is generally of medium importance, reflecting the diverse decay heat removal methods in the BWR design, and the long recovery period available for restoration of unavailable systems. Millstone has been assessed a higher importance for this sequence, primarily because of limitations in support system redundancy. The loss of key support system components (i.e., an emergency AC power source) seems to have a greater impact on decay heat removal than at other plants. The Peach Bottom and Grand Gulf PRAs do not have any contribution to this sequence.

### 4.3 Representative Accident Sequence 3: Station Blackout with Intermediate Term Failure of High Pressure Injection

#### Sequence Description

Representative Sequence 3 is initiated by a loss of offsite power or, to a lesser extent, by a transient with a subsequent LOOP.

The sources of emergency AC power, i.e., the emergency diesel generators (EDGs) fail primary due to EDG hardware failures. Maintenance unavailability is a secondary contributor. Support system malfunctions include: EDG room and battery/switchgear room HVAC failures and service water pump or EDG jacket cooling water hardware failures.

The loss of all AC power to a Unit's emergency buses is called a station blackout (SBO). The definition of a station blackout in terms of EAC unavailability can vary depending on the emergency bus distribution design. In general, SBO assumes the failure of all the diesels that support long term decay heat removal. In the case of a single unit (Grand Gulf) or multiple units with separate EAC power sources (Millstone Unit 1) the loss of two sources of emergency AC power is defined as a SBO.<sup>6</sup> Multi-unit sites with shared EDGs typically require more failures to disable the decay heat removal function. At Peach Bottom a SBO is defined as the loss of all four diesels. In general, the fewer the sources of emergency power the more important single component failures or EDG unavailability can become. Conversely, multiple EAC sources are more vulnerable to common failure modes including support system failures.

Some of the input sequences postulate HPCI or HPCS loss due to random failures, however, in all cases some HPI system is available. The high pressure injection systems provide core makeup until the station batteries are depleted or the injection fails due to environmental conditions, primarily high suppression pool temperature.

#### Plant Specific Design Operating Insights

As shown in Table 3.4, the plant specific core damage frequency contributions associated with sequence 3 vary widely from less than 1% (Millstone Unit 1) to 81% for Grand Gulf. This sequence postulates failure of RPV injection due to battery depletion (4-12 hours) or high suppression pool

---

<sup>6</sup> Grand Gulf has Division 3 emergency AC power with a dedicated EDG, which provides power to a HPCS system. NUREG/CR 4550 for Grand Gulf, Unit 1 defines a SBO as the loss of emergency AC Divisions 1 and 2, but not Division 3.

temperatures in 6-8 hours after the loss of all AC power. Without AC power recovery, the loss of makeup results in core damage. Most BWRs utilize HPCS/HPCI and the RCIC systems for SBO coping. The turbine driven systems are dependent on DC power, and all utilize self-cooled pumps that depend on moderate pool temperatures for continued operation. Millstone has an isolation condenser for long term decay heat removal under SBO conditions. The isolation condenser does not have the same dependencies as the aforementioned HPI systems and the Millstone vulnerability to SBO is dominated by the immediate failure of the IC, as addressed in representative accident sequence 4.

The major contributor to this sequence is the failure of emergency AC power. This is dominated by the failures of all EDGs to start or run, test and maintenance unavailability and failure of the EDG support systems. Single unit sites generally have two EDGs that must fail to cause a SBO. The operation of a HPCS EDG (if applicable) is not sufficient to avoid SBO.

- Multi-unit sites with dedicated EDGs frequently have hardwired, administratively controlled bus cross-ties that provide significant flexibility. For example, the unit 1 EDGs may be able to power safety equipment on unit 2 buses.
- The Peach Bottom site has four shared diesels. This arrangement generally provides the most flexibility as all four diesels must be unavailable to cause a SBO. However, as noted below the interrelationship among EAC support systems must be established to realize maximum redundancy.

The major plant design features that can influence plant vulnerability to this sequence are:

- The service water (SW) system provides EDG jacket water cooling. The diversity of this support system contributes to the relative importance of SW to this sequence. A design that allows multiple train cooling to each EDG is less vulnerable to SW induced EDG failures than a strictly divisional configuration.
- Some service water system operating modes may have common discharge lines with normally open MOVs or single booster pumps, which can have a significant impact on system availability.
- The four Peach Bottom EDGs are not completely independent due to service water system interdependencies. Depending on the SW system success criteria, the failure of two EDGs (IREP modeling) or three EDGs (utility modeling) will fail cooling to the remaining EDG(s) and cause SBO.

#### Qualitative Estimate of Sequence Importance

With the exception of Millstone, this sequence is highly important for the representative plants. As discussed above, the multi unit sites normally have significant EAC diversity due to hardwired bus cross-ties and/or electrical bus diversity within a plant. However, these potential advantages have not been fully credited in the reference PRAs due to simplifying assumptions or conservative system success criteria interpretations.

The SW system is important in this sequence as a support system to the EDGs. System designs that have multiple SW trains to each diesel make EAC power less vulnerable to single SW pump or valve failures.

#### 4.4 Representative Accident Sequence 4: Station Blackout with Short Term Failure of High Pressure Injection

##### Sequence Description

This sequence is initiated by a loss of offsite power, or to a lesser extent, by a transient with a subsequent LOOP. The sources of emergency AC power i.e., emergency diesel generators (EDGs) fail primarily due to hardware failures. Secondary contributors are output breaker failures and EDG unavailability due to test or maintenance (T&M). Support system malfunctions also contribute to the loss of all AC power. Service water hardware failures in the EDG jacket cooling water train, battery/switchgear room HVAC failures and HVAC T&M unavailability are significant support system contributors to EDG unavailability. As discussed below DC power failures are also important.

Unlike a classic station blackout with injection failure upon station battery depletion, this sequence postulates short term failures of HPI or the DC batteries. HPI system malfunctions include pump hardware failures and system maintenance unavailability. DC battery failures (including common mode) are most significant, because both the high pressure injection systems and the EDGs require DC power.

Core damage generally occurs less than one hour after the failure of all injection systems.

##### Plant Specific Design Operating Insights

The plant specific contributions to representative accident sequence 4 are significant for the reference plants with the exception of Plant B. This plant's electrical distribution design powers several major LPCI components from the opposite unit's EDGs. This feature allows RPV injection despite a failure of one unit's EDGs and HPI systems.

The large Peach Bottom contribution to this sequence is driven by an assessed common mode battery failure of five of the eight plant battery buses. This, in turn, disables all EDGs, HPCI, RCIC and the SRVs. The modeling of potential common mode failures is subject to considerable uncertainty because of sparse data. The Peach Bottom EDG arrangement and its service water support has been discussed in sequence 3.

In addition to the DC power system, EAC and HPI are major contributors to sequence 4. The emergency AC power system has been discussed in sequence 3. The contributing Grand Gulf sequences postulate failure of the HPCS EDG or random HPCS failures. Given a loss of offsite power, the total HPCS unavailability (including EAC support) is comparable to a HPCI system. The Millstone HPI redundancy is more limited than most, because under SBO conditions all vessel injection systems are inoperable. However, the isolation condenser can provide core decay heat removal independent of AC power.

##### Qualitative Estimate of Sequence Importance

Regardless of the PRA modeling issues, it is important to note that the Peach Bottom DC power system does not have any unusual characteristics that would adversely differentiate it from the



rest of the GE BWRs. Given the extensive dependence of BWR systems on DC power, a common mode failure of the station batteries is a major contributor to core damage frequency. Since BWRs (including Plant B) appear vulnerable to this failure, representative accident sequence 4 is judged to be highly important for all of the reference plants.

#### 4.5 Representative Accident Sequence 5: ATWS with Failure of RPV Water Level Control at High Pressure

##### Sequence Description

Representative Sequence 5 is a general transient with initial or subsequent MSIV closure and a failure of the RPS. Attempts to manually scram are also not successful. The standby liquid control (SLC) system is subsequently initiated. This sequence postulates a failure to control RPV water level at high pressure.

The high pressure injection (HPCS/HPCI) system fails, primarily due to pump failure to start or T&M unavailability. Injection or minflow valves, suction switchover or loss of DC power are other system failures.

At this point, HPCI (or HPCS) has failed and ADS is inhibited. The remaining high pressure injection systems cannot keep the core covered at ATWS power levels. The operator fails to manually depressurize in a timely fashion, and core damage ensues.

##### Plant Specific Design Operating Insights

The PRA modeling of ATWS sequences is complex, continually evolving and subject to uncertainty. This is reflected in the plant specific contributions to this representative accident sequence which range from <1% (Plant A) to 19% (Plant B). The four reference PRAs with accident sequence cutsets were examined in detail. With the possible exception of the HPI, the major hardware contributions (i.e., transient initiator frequency and RPS failure rates) are similar among the plants.

The individual plant specific contributions to this sequence are dominated by the different success criteria for RPV level control. This is somewhat attributable to the evolving nature of BWR ATWS mitigation. For example:

Millstone does not contribute to this sequence because the IREP was completed before the BWROG EPG philosophy of ATWS level/power control was adopted.<sup>7</sup>

The Plant B PRA assumes a 43 gpm (pre-ATWS Rule) SLC injection capacity. This assumption affects the success criteria for level control which requires that the operators maintain a narrow RPV level band around the top of the active fuel (TAF). Based on ATWS computer modeling with a 43 gpm SLC capacity, if RPV water level is maintained too high, excessive core power production causes high suppression pool temperature. This high suction temperature is assumed to fail high pressure injection prior to the injection of sufficient sodium pentaborate to cause hot shutdown. The

---

<sup>7</sup> The BWR Owners' Group Emergency Procedure Guidelines direct the operator to lower RPV water level until the reactor power level drops below the average power range monitor downscale trip, or reactor water level reaches TAF, or all SRVs remain closed and drywell pressure remains below the scram setpoint.

Plant B PRA also conservatively assumes that the operator will fail to depressurize and align low pressure injection given ADS is inhibited and HPI fails. The relatively high Plant B contribution to this representative accident sequence is a direct result of those stringent water level control success criteria.

The ATWS rule (10CFR50.62) requires an enhanced SLC injection rate "equivalent in control capacity to 86 gpm of 13 weight percent sodium pentaborate solution" for each BWR. The Peach Bottom and Grand Gulf PRAs took credit for the 86 gpm equivalent SLC injection rate. ATWS computer simulations for Peach Bottom showed if the SLC system is initiated within four minutes, the reactor would be shutdown prior to reaching high pool temperatures even without manual water level control. These risk assessments define a failure to control water level at high pressure as manual control of reactor vessel water level that is too low and causes core damage. Automatic HPI level control (between levels 2 and 8) is considered a success. This success criterion results in a very low assessed failure rate for ATWS water level control at high pressure.

The major hardware variation among the contributing reference plants is the systems used for high pressure injection during ATWS. As previously discussed, the composite transient initiator for this sequence has a relatively small LOOP contribution (approximately 2%). Within the context of this sequence, given the availability of offsite power, the motor driven HPI systems (such as HPCS) are considered to be more reliable than their turbine driven counterpart (HPCI).

#### 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 5. The individual plant contributions to this sequence are driven by PRA modeling assumptions. The comparative reliability of high pressure injection systems is somewhat less important.

#### 4.6 Representative Accident Sequence 6: ATWS With Failure of RPV Water Level Control at Low Pressure

Representative Sequence 6 is a general transient with Reactor Protection System (RPS) failure. Attempts to manually scram also fail. MSIV closure results in the loss of the condenser. SLC injection is successful. In order to minimize SRV discharges to the suppression pool the operator lowers RPV water level. At this point, the sequence branches.

1. The operator fails to inhibit ADS. RPV water level is being controlled below the ADS logic setpoint. Automatic depressurization occurs, followed by uncontrolled low pressure injection.
2. The operator inhibits ADS. The high pressure injection sources fail to supply sufficient makeup. The RPV is manually depressurized to allow low pressure injection. The operator fails to control water level using the low pressure systems.

The failure of RPV water level control results in increased reactor power, increased suppression pool temperature and pressure. The containment fails due to overpressure which fails all RPV injection from the suppression pool, and results in core damage.

### Plant Specific Design Operating Insights

As stated previously, ATWS modeling has considerable uncertainty. The BWR Owner's Group Emergency Procedure Guidelines (EPGs), the enhanced SLC control capacity and advances in thermal hydraulic codes have influenced success criteria and mitigation techniques.

Once again, the evolutionary nature of the BWR ATWS response has resulted in varying contributions to this sequence. The four PRAs with accident sequence cutsets were examined in detail. The plant configuration and ATWS modeling vary, due to the regulatory environment and mitigation techniques in effect during the development of the PRA, as discussed below:

The Millstone 1 IREP does not contribute to this sequence because it was completed before the adoption of the BWROG Emergency Procedure Guidelines ATWS power and level control guidance. The 43 gpm (pre-ATWS Rule) SLC injection capacity<sup>8</sup> as modeled in the Plant B PRA is the primary reason for the large (16%) contribution to this representative sequence.

The original SLC system configuration requires an extended time period (15-30 min) (Ref. 4) for the injection of the hot shutdown boron weight. In the interim, the suppression pool temperature increases, and the RPV is depressurized in conformance with the heat capacity temperature limits of the emergency operating procedures. The 43 gpm SLC capacity results in a higher ultimate pool temperature and a lower RPV pressure. These factors combine to make continued HPI unlikely to occur. The Plant B ATWS modeling assumes eventual manual depressurization and switch over to low pressure injection. Twelve of the sixteen percent that Plant B contributes to this sequence (see Table 3.4) can be ascribed to the subsequent failure to maintain level within one foot of the top of the active fuel (TAF). The remainder of the Plant B contribution to this sequence is attributable to the failure of water level control at low pressure given a previous HPI failure or an inadvertent ADS actuation.

Grand Gulf and Peach Bottom do not contribute to this representative sequence because the enhanced SLC injection capacity of 86 gpm, equivalent was credited in these PRAs. The increased injection rate is expected to allow reactor shutdown prior to the loss of the high pressure injection systems. These PRAs do have sequences that postulate automatic depressurization or HPCS/HPCI system failures that require the low pressure systems. However, the success criteria for low pressure level control requires that RPV level be maintained no lower than six feet below TAF. Potential power excursions or boron dilution due to vessel overfill appear to be neglected. Consequently, these PRAs have a very low failure estimate for low pressure level control.

In addition to the relatively higher reliability of the HPCS system (see sequence 5) the ADS inhibit switch is an important plant design feature. On the basis of simulator observations, an MSIV closure with ATWS requires that the operators perform multiple tasks within a short time period. The inhibit switch (Peach Bottom, Plant B) eliminates the periodic manual resetting of the ADS (Grand Gulf) and reduces the potential for inadvertent system actuation.

---

<sup>8</sup> The plant SLC injection capability has since been upgraded to conform to the requirements of 10CFR50.62.

### Qualitative Estimate of Sequence Importance

Plant specific contributions to sequence 6 are largely determined by modeling assumptions, rather than the HPI and ADS design variations, noted above. On this basis, the reference plants have been assigned a medium importance for representative accident sequence 6.

#### 4.7 Representative Accident Sequence 7: ATWS with Failure of Standby Liquid Control (SLC) Injection

Representative sequence 7 is a general transient with failure to scram. Manual scram is also not successful. The majority of the contributing sequences (84%) assume PCS isolation. The focus of this sequence is the failure of the SLC system. The estimated unavailability of the SLC system is dependent on the compliance alternative that was adopted to meet the 86 gpm equivalent injection requirement of the ATWs Rule (10CFR50.62).

The enriched boron option maintains the original system design. The increased control capacity is obtained by using sodium pentaborate that contains approximately 40 atom percent of the Boron 10 isotope. This isotope is the neutron absorber and normally accounts for 19.8 atom percent of the naturally occurring boron. The enriched boron option allows the SLC to retain its redundancy. Consequently, human errors such as the failure of timely SLC initiation or the failure to restore the system after testing dominate system unavailability.

The two pump alternative simultaneously uses both SLC pumps to inject natural pentaborate (19.8% B<sup>10</sup>) into the reactor vessel. This configuration eliminates the system redundancy as both pump trains must be operable to meet the higher injection requirement. As expected, hardware failures become more important, accounting for approximately 50% of system unavailability. An additional contributor is the failure of the Reactor Water Cleanup (RWCU) isolation valve to close on SLC actuation.

As the sequence progresses, the continued RCS blowdown (even with adequate water level control) causes suppression pool heatup. Depressurization due to the heat capacity temperature limit (HCTL) or the high pool temperature itself fails high pressure injection. Failures of water level control at high or low RCS pressure accelerate containment pressurization and the onset of core damage.

#### Plant Specific Design Operating Insights

Once again, the success criteria definitions determine the plant specific contributions to this sequence. Most plants assume that the failure of timely SLC initiation (i.e., within four minutes) results in core damage. The human error probability (HEP) associated with the system initiation is not negligible and, depending on the SLC compliance alternative, can be a major cause of system failure. The Grand Gulf PRA has a different approach. The SLC initiation HEP is extremely low, and the plant utilizes two pump injection which would normally be expected to have a considerable hardware contribution. However, the PRA assumes that given SLC failure, the level/power oscillations do not damage the core and containment failure does not result in the loss of RPV injection. On this basis, the Grand Gulf PRA has a very small contribution to this representative sequence which is due to random injection failures, not SLC unavailability.

Although it is not reflected in the reference PRAs, plants that use the two pump SLC configuration are generally expected to have a higher contribution to representative accident sequence 7 because of the higher estimated unavailability of this non-redundant arrangement.

#### Qualitative Estimate of Sequence Importance

This sequence is considered to be of medium importance for the reference plants on the basis of plant specific contributions (Table 3.4) and a detailed PRA review. A higher importance may be appropriate for those plants that utilize a two pump SLC injection configuration, in conjunction with a limited suppression pool mass (typically associated with Mark I and some Mark II containments). A large suppression pool thermal capacity can provide a potential success path in the event one of the two SLC trains is unavailable.

#### 4.8 Representative Accident Sequence 8: Unisolated LOCA Outside Containment

The initiator is a large pressure boundary failure outside containment with a failure to isolate the rupture. The piping failure is postulated to occur in the following systems: main steam (50%), feedwater (10%), high pressure injection (33%), and interfacing LOCA (7%). An interfacing systems LOCA initiator (ISLOCA) is defined as the initial pressurization of a low pressure line which results in a pressure boundary failure, compounded by the failure to isolate the break. The failure is typically postulated in a low pressure portion of the core spray (CS) system, the LPCI, shutdown cooling, and (to a much lesser extent) the head spray line of RHR systems. Human error was an important contributor to recent events at a Mark I BWR in which the RCIC suction piping was overpressurized during testing while at power. Plants with isolation condensers can have tube or tube sheet failures and low pressure RWCU systems are also subject to interfacing system LOCA concerns. Unlike most BWRs, the Millstone SDC system is designed for RCS pressure and does not contribute to this sequence. The importance of the interfacing LOCA is influenced by two factors.

- On line surveillance of the high to low pressure interface valves for the CS and RHR valves could raise the importance of this sequence.
- Several BWRs have performed analyses to confirm the pressure retaining capability of the low pressure piping under interfacing LOCA conditions.

The unisolated LOCA outside containment results in a rapid loss of the reactor cooling system (RCS) inventory. Piping failures in the reactor building can result in unfavorable environmental conditions for the ECCS in addition to the depletion of the finite suppression pool inventory. Ruptures outside the reactor building cause minimal ECCS impact which can enable manual realignment of the ECCS suction to the condensate storage tank. The condensate system can also be used for primary system makeup for most of these initiators.

#### Plant Specific Design and Operating Insights

The plant specific core damage frequencies associated with representative sequence 8 are very low. Unlike PWRs, the LOCA outside containment sequence is not a significant contributor for any of the BWR PRAs examined. This is attributable, in part, to the lower RCS operating pressure which reduces the interfacing system (ISLOCA) contribution. Several BWRs have performed analyses to confirm the integrity of the low pressure piping under interfacing systems LOCA conditions.

The major systems that contribute to LOCA outside containment do not vary significantly among BWRs. In general, the number and arrangement of the containment isolation valves, piping sizes and lengths, and the available mitigation systems are fairly consistent. However, there are two notable low pressure interface design features.

The most common low pressure ECCS interface design has an air operated check valve inside containment, a normally closed motor operated outboard containment isolation valve, and an upstream (further from containment) normally open MOV at the interface boundary. Peach Bottom and Grand Gulf have an interlock that prevents both MOVs from being open at the same time. This can significantly reduce plant risk due to the on-line testing of the interface valves. Other plants, such as Millstone, have additional normally closed MOVs or check valves within the high pressure piping that must also fail in order to challenge the upstream low pressure piping.

Given the relative similarity of the GE BWRs, the major influence on plant specific exposure to ISLOCA is operating practices. For example, Plant B racks out the breakers for the SDC interface MOVs as a backup to the valve pressure interlocks. In addition, on line testing of the high to low pressure interface valves for the RHR and CS systems can dramatically increase the importance of this sequence.

#### Qualitative Estimate of Sequence Importance

Representative accident sequence 8 generally has a low importance from a core damage perspective. However, on the basis of health effects the sequence is more significant. The limited response measures to a LOCA outside containment, in conjunction with the high level of design consistency among BWRs, means that plant specific operating practices are the primary determinant of sequence importance. In particular, plants that have on line testing of the LPI interface valves (Peach Bottom, Millstone) can increase the interfacing system LOCA core damage frequency by up to two orders of magnitude. Although interface MOV interlocks can significantly reduce the initiator frequency, plants might want to analyze the risk-benefits of on line interface valve testing for BWRs. Alternatively, the test procedures should incorporate industry experience to reduce the potential for ISLOCA.

Table 4.1 Representative Sequence Priorization Summary<sup>1</sup>

Repres. Sequen.	Ref. Plant	Sequen. Import.	Qualitative Success Estimate for Critical Functions and Systems														
			ADS	HPI	SW	RHR	IC	EMERG. AC POWER	DC POWER	RPS	ADS INHIBIT	LPI	SLC	LPI <sup>2</sup> INTER INTEG	SDC <sup>2</sup> INTER INTEG		
1	Millstone Plant B Peach Bottom Grand Gulf	High Medium Medium	Lower Average Average Lower	Lower Average Average Higher													
2	Millstone Plant B Peach Bottom Grand Gulf	High Medium 3			Higher Average	Lower Average											
3	Millstone Plant B Peach Bottom Grand Gulf	Low High High High			Average Higher Lower Average		Average N/A <sup>4</sup> N/A N/A	Average Average Higher Average									
4	Millstone Plant B Peach Bottom Grand Gulf	High High High High		Lower Average Average Higher	Average Higher Lower Average		Average N/A <sup>4</sup> N/A N/A	Average Average Higher Average	Average Average Average Average			Average Higher Average Average					
5	Millstone Plant B Peach Bottom Grand Gulf	3 Medium Medium Medium		Average Average Higher							Average Average Average						
6	Millstone Plant B Peach Bottom Grand Gulf	3 Medium Medium Medium		Average Average Higher							Average Average Average	Average Average Lower	Average Average Average				
7	Millstone Plant B Peach Bottom Grand Gulf	Medium Medium Medium Medium									Average Average Average Average			Average Average Average Lower			
8	Millstone Plant B Peach Bottom Grand Gulf	Low Low Low Low														Lower Average Lower Higher	Higher Higher Average Average

<sup>1</sup> See the text for a discussion of critical function and system availability.  
<sup>2</sup> Low pressure injection (LPI), shutdown cooling (SDC), low to high pressure interface integrity.  
<sup>3</sup> No sequence based information is available in the reference plant PRA.  
<sup>4</sup> N/A, not applicable

## 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 strict 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 mathematics for calculating the average basic event importances are presented in Section 5.1. The importance measure is a relative measure of risk in terms of core damage and can be used to prioritize the basic events for inspection purposes.



Each representative accident sequence can envelope multiple plant-specific sequences from each of the four reference PRAs. Basic event importance values ( $I_i^b$ ) are calculated and subsequently normalized for each of the plant-specific accident sequences (Eq. 5-1). The average basic event importance ( $I^A$ ) of Table 5.1 is simply the average of the contributing plant-specific normalized importance value ( $I_i^p$ ), as shown by Eq. 5-2.

These 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 the average importance, may de-emphasize the risk significance of certain plant-specific variations. The plant-specific modifiers (Section 5.2) were developed to approximate the risk significance of selected basic events. They are applied where a significant deviation between the average importance value of Table 5.1 and the corresponding plant-specific value occurs that is attributable to plant-specific design or operating features. Section 5.2 provides a simple example for illustrative purposes.

Section 5.3 briefly discusses a system-oriented approach or inspection matrix that is presented in Appendix A. This matrix is a plant activity based organization of the basic events for the representative accident sequences.

#### 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 for each plant-specific sequence, so that the summation of these average 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. Therefore, an average basic event importance was calculated for each basic event in the representative accident sequence by taking the summation of all the normalized basic event values for that same event in the pertinent plant-specific sequences, and then dividing by the total number of plant-specific sequences contributing to the representative sequence.

Mathematically, the above discussion can be represented as follows:

$$I_t^P = \frac{I_t^I}{\sum_{i=1}^m I^I(i)} \quad (5-1)$$

where

- $I_t^I$  = the Inspection Importance of the  $l$  basic event for a plant specific sequence
- $m$  = the number of basic events in a plant specific sequence
- $I^I(i)$  = the inspection importance of basic event  $i$
- $I_t^P$  = the normalized importance for basic event  $l$  of a plant specific sequence

To calculate the average importance of the basic events in the representative sequences, each of the normalized basic event importances,  $I_t^P$ , are then substituted into the following equation

$$I_t^A = \frac{1}{n} \sum_{i=1}^n I_t^P(i) \quad (5-2)$$

where:

- $I_t^A$  = 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 ADS human error, "Failure to manually depressurize using non ADS valves."

The plant specific contributors to Sequence 1 are:

<u>Plant</u>	<u>PRA Specific Sequence No.</u>	<u>Total No. of Sequences</u>
Millstone (IREP)	1,3,5	3
Plant B	4,15,22	3
Peach Bottom	A	1
Grand Gulf	-	0
		N = 7

The basic event Inspection Importance for this particular human error, event  $\ell$  is:

<u>Plant</u>	<u>PRA Specific Sequence No. Containing Event <math>\ell</math></u>	<u>Normalized Inspection Importance for Event (<math>I_i^P</math>)</u>
Millstone	1	20
	3	20
	5	20
Plant B	None	-
Peach Bottom	A	12
		-----
		$\Sigma I_i^P = 72$

The average basic event importance,  $I_i^A$ , is then:

$$I_i^A = \frac{1}{n} \sum I_i^P = \frac{1}{7}(72) \approx 10$$

## 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). The average importance values are a composite of the reference plant design system redundancy, operational practices and other features. The PSM approximates the contribution of these plant-specific variations.

A total of 30 modifiers are provided in Table 5.1. They are intended to accommodate the various design and operating variations in GE plants. The events in Table 5.1 are cross-referenced to the applicable modifiers. Plant specific basic event importances for plants can be derived using these modifiers. These modifiers judgementally reflect, the design/operating variations from the four reference plants (Millstone, Plant B, Peach Bottom and Grand Gulf ).

As an example, for the same basic event mentioned in Section 5.1, PSM No. 17 is cross-referenced in Table 5.1 The factor of 2 (PSM No. 17) was developed in the following way. In the Millstone IREP, there were 3 contributing sequences to Representative Sequence No. 1., i.e., Nos. 1,3,5. All three contained the basic event. Hence, the Average Inspection Importance for this event, considering only Millstone is:

$$I_t^A = \frac{20+20+20}{3 \text{ sequences}} \approx 20$$

versus the average for all plants,  $I_t^A = 10$ . The intent of the plant specific modifier (PSM) is to approximate the contribution this basic event would make in a plant with a configuration similar to Millstone. Hence, the applicable PSM (No.17) is:

$$PSM = \frac{20}{10} = 2$$

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. The last column of Table 5.1 provides these PSM notes to identify the applicable PSM for the corresponding basic events. The PSMs are listed sequentially following Table 5.1.

### 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 eight 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**

*BWR Representative Accident Sequence 1 - Loss of High Pressure Injection and Failure to Depressurize*

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
<b>INITIATOR</b>		
Transients w/immediate or subsequent loss of PCS	20	3
Loss of offsite power (LOOP) initiator	2	3,4
	Initiator total = 22	
Stuck open relief valve (SORV)	6	19
<b>RECOVERY</b>		
Failure to recover offsite power	2	4, 5
Failure to recover PCS	9	5
	Recovery total = 11	
<b>ADS/MANUAL DEPRESSURIZATION</b>		
• Human Error Failure to manually depressurize using non ADS valves	10	17
• Hardware ADS valve fails to open incl. ADS common cause failure due to O-ring leakage	12	
	ADS total = 22	
<b>HIGH PRESSURE INJECTION (HPI)</b>		
<b>HPCI/HPCS</b>		
• Pumps HPI pump fails to start or run	8	20
HPI pump in test or maintenance	2	20
	HPCI/HPCS sub-total = 10	

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.

**Table 5.1 (Cont'd)**

*Sequence 1 (cont'd.)*

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
<b>RCIC</b>		
• Pumps		
RCIC pump fails to start or run	4	
RCIC pump in test or maintenance	2	
RCIC sub-total = 6		
<b>CRD Hydraulic System</b>		22
• Human Error		
Operator fails to manually start and align the second CRD pump	2	
Operator fails to align CRD hydraulic system valves to maximize RPV injection	1	
• Pumps		
CRD pump fails to start	<1	
CRD pump in maintenance	<1	
CRDH sub-total = 3		
<b>Feedwater Coolant Injection (FWCI)* System</b>		
• Hardware		
Failure of FWCI pump breaker	1	
FWCI pump pressure permissive switches fail	<1	
FWCI pump pressure permissive switch out for test or maintenance	<1	
• I&C		
FWCI initiation logic fails	<1	
• FWCI Support Systems		
Mechanical failure of SWS to provide cooling to the FWCI pump	1	
Failure of the cond transf to provide makeup to FWCI	1	
FWCI sub-total = 3		
HPI total = 21		

\*BWR 3 only

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.

**Table 5.1 (Cont'd)**

*Sequence 1 (cont'd.)*

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
<b>HVAC</b>		
• Recovery Failure to recover HVAC to switchgear room	2	
• Hardware DG bldg HVAC to a switchgear room fails, disabling a bus	4	
HVAC total = 6		
<b>AC POWER</b>		
• Hardware Breaker failure prevents the loading of the emergency generator	2	10
Emergency generator fails to start or run	2	10
AC total = 4		
<b>ISOLATION CONDENSER (IC)*</b>		
• Human Error Operator fails to open IC makeup valve	1	
• Hardware Failure of isolation condenser makeup valve to open	2	
Isolation Condenser isolation valves closed for test or maintenance	2	
• I&C Isolation condenser initiation logic relay contacts fail to operate	1	
IC total = 6		

\*BWR 3 only

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.

**Table 5.1 (Cont'd)**

***BWR Representative Accident Sequence 2 - Loss of Containment Heat Removal***

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
<b>INITIATOR</b>		
Transient with immediate or subsequent loss of PCS	21	3
LOOP	2	3,4
Initiator total = 23		
Stuck open relief valve (SORV)	4	19
<b>RECOVERY</b>		
Failure to:		
- successfully vent the containment	15	7,8
- recover offsite power	2	4,7
- reestablish the power conversion system (PCS)	10	7
- recover IC makeup by manually opening valve	4	9
- recover RHR failed valve	3	7,23
Recovery total = 34		
<b>SERVICE WATER (SW)</b>		
• Valves		
Common cause failure of SW valves disables both RHR HXs	<1	
• Pumps		
Service water pump(s) fail to run	10	23
• Heat Exchangers (HXs)		
RHR HX unavailable due to SW testing or maintenance	5	23
RHR HX fails due to plugging on the SW side	2	23
SW total = 17		

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.



Table 5.1 (Cont'd)

Sequence 2 (Cont'd.)

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
<b>EMERGENCY AC POWER</b>		
Emergency generator fails to start or run	4	11
Generator breaker fails to close	4	11
EAC Power total = 8		
<b>INSTRUMENT AC</b>		
Transformer/breaker malfunctions that fail instrument AC and pump cooling for the LPCI containment cooling modes and the control logic for shutdown cooling	5	15
Instrument AC auto bus transfer fails disabling instrument AC with the same consequences as above	3	15
IAC total = 8		
<b>RESIDUAL HEAT REMOVAL (RHR)</b>		
• Valves		
RHR min flow valve(s) fail to open on demand, including common mode	1	23
RHR HX bypass valve(s) fail to close including common mode	1	23
RHR suppression pool return valve(s) fail to open including common mode	1	23
Plugging of RHR suppression pool strainer	1	24
RHR loop unavailable due to testing or maintenance	1	23
RHR total = 5		

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.

**Table 5.1 (Cont'd)**

***BWR Representative Accident Sequence 3 - Station Blackout with Intermediate Term Failure of High Pressure Injection***

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
<b>INITIATOR</b>		
Loss of offsite power (LOOP) initiator	16	
Transient initiator w/subsequent LOOP	3	
Initiator total = 19		
<b>RECOVERY</b>		
Failure to recover offsite power	20	6
Failure to recover from EDG hardware failure including common mode	12	6
Failure to recover from EDG maintenance outage	2	6
Recovery total = 34		
<b>EMERGENCY AC POWER (EAC)</b>		12
EDG fails to start or run (incl. common mode)	34	
EDG in maintenance	4	
EDG actuation logic failure	<<1	
EAC total = 38		
<b>SERVICE WATER (SW)</b>		
• Human Error		
Operator fails to manually start SW booster pump to cool EDGs	3	
• Valves		
SW common inlet or return valve to EDG jacket cooler in maint.	<1	
• Pumps		
SW pump hardware failure (failure to start/run) disables EDG cooling	3	26
SW pump out for maintenance	1	26

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.

**Table 5.1 (Cont'd)**

**Sequence 3 (Cont'd)**

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
<b>• General</b>		
SW EDG jacket cooling HX train fails (primary jacket water HX inlet or outlet valves)	4	27
SW EDG HX train (primarily jacket cooler HX) out for maint.	<1	
Common mode failure of SW trains fails all EDG cooling	<1	
SW total = 8		
<b>HVAC</b>		
EDG room HVAC hardware failing (incl. fan, damper failures)	1	
Battery/switchgear room HVAC hardware failure disables one AC and/or DC division	1	
Battery/switchgear room HVAC in maintenance	<1	
EDG room HVAC out for maintenance	<1	
HVAC total = 2		
<b>DC POWER</b>		
Battery Failure	<1	
Battery charger failure	<1	
DC Power total = <1		

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.

**Table 5.1 (Cont'd)**

***BWR Representative Accident Sequence 4 - Station Blackout with Short Term Failure of High Pressure Injection***

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
<b>INITIATOR</b>		
Loss of offsite power (LOOP)	21	
Transient with subsequent LOOP	4	
Initiator total = 25		
Stuck open relief valve (SORV)	3	19
<b>RECOVERY</b>		
5		
Failure to recover:		
- offsite power	13	
- battery/switchgear cooling	3	
- from EDG hardware faults	1	
- a battery fault	1	
- from EDG maint. unavailability	<1	
Recovery total = 18		
<b>EMERGENCY AC POWER</b>		
13		
EDG hardware fault (incl. common mode failures)	14	
Breaker fails to close preventing energizing the bus	2	
LOOP trip signal fails to reset, EDGs unable to pick up load	4	14
EDG unavailable due to maintenance	1	
Loss of EDG actuation signal incl. relay failure	<1	
EAC power total = 21		
<b>DC POWER</b>		
Failure of a battery (incl. common mode)	18	16
DC battery unavailable due to maint.	<1	
DC Power total = 18		

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.

Table 5.1 (Cont'd)

Sequence 4 (Cont'd)

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
--------------------------	-----------------------------------------	-------------------------------------

**HVAC/ROOM COOLING**

Battery/switchgear room cooling failures causes the loss of a switchgear train	3	
Battery/switchgear room cooling train unavailable due to maintenance	2	
EDG room HVAC (room cooler) hardware failures	<1	
EDG room HVAC in maintenance	<<1	

HVAC/Room Cooling total = 5

**HIGH PRESSURE INJECTION (HPI)**

**HPCI/HPCS**

• Valves

Condensate storage tank outlet valve plugged, also fails RCIC	<1	
Min flow valve fails to open (incl. controller failures)	<1	

• Pumps

Pump hardware failure (failure to start)	1	21
------------------------------------------	---	----

• I&C

Suppression pool switchover logic fails	<1	
Actuation logic fails	<1	

• General

System unavailable due to maintenance including TDP	<1	
Injection line hardware failure (primarily valves)	<1	

HPCI/HPCS sub-total = 1

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.

**Table 5.1 (Cont'd)**

**Sequence 4 (Cont'd)**

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
<b>RCIC</b>		
• Human Error Operator fails to manually start RCIC given auto actuation failure	<<1	
• Valves Min flow valve fails to open (incl. controller failures)	<1	
Steam inlet valve (at turbine) fails to open	<1	
Steam line containment isolation valve fails to open	<1	
RCIC injection line valve failure (near feedwater/RCIC interface)	<1	
• Pump Pump fails to start or run	2	
• General RCIC system unavailable due to maint.	1	
RCIC lube oil cooler hardware failure	<1	
• I&C RCIC actuation logic fails	<1	
	RCIC sub-total = 3	
	HPI total = 4	
<b>ISOLATION CONDENSER (IC)*</b>		
Failure to recover IC makeup by manually opening failed valve	2	25
IC isolation valves not restored after test or maintenance	1	25
	IC total = 3	

**\*\*BWR3 only**

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.

Table 5.1 (Cont'd)

*Sequence 4 (Cont'd)*

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
<b>SERVICE WATER (SW)</b>		
• Human Error		
Operator fails to manually start SW booster pump to cool EDGs	<1	
• Pumps		
SW pump hardware failure	1	26
SW pump out for maintenance	<1	26
• General		
SW EDG jacket cooling HX train fails (primarily jacket water HX inlet or outlet valves)	2	27

SW Total = 3

**REACTOR PRESSURE VESSEL (RPV) LEVEL INSTRUMENTATION**

Common mode miscalibration	<<1
----------------------------	-----

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.

Table 5.1 (Cont'd)

*BWR Representative Accident Sequence 5 - ATWS with Failure of RPV Water Level Control at High Pressure*

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
<b>INITIATOR</b>		
General transient with initial or subsequent MSIV closure	25	3
<b>SCRAM FUNCTION</b>		
Failure of RPS and manual scram	25	
<b>REACTOR PRESSURE VESSEL (RPV) WATER LEVEL CONTROL</b>		
Operator fails to manually depressurize RPV (given HPCI/HPCS failure and ADS inhibited). The remaining high pressure systems cannot keep core the covered	25	
<b>HIGH PRESSURE INJECTION (HPCI or HPCS)</b>		
• Valves		
Min flow valve fails to open incl. controller	2	
Injection line valve near FW interface (or at RPV for HPCS) fails to open	2	
Steam inlet valve (at turbine) fails to open	<<1	
• Pump		
HPI pump fails to start or run	14	20
HPI pump unavailable due to test or maint.	6	20
• I&C		
HPI suction switch over logic fails	1	
HPI actuation train fails	<1	
HPCI level switch at steam line drain pot fails (no output)	<1	
Lube oil cooling fails	<<1	

HPI total = 25

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.



Table 5.1 (Cont'd)

*Sequence 5 (Cont'd.)*

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
<b>DC POWER</b>		
Loss of DC power from one station battery	<<1	
<i>BWR Representative Accident Sequence 6 - ATWS with Failure of RPV Water Level Control at Low Pressure</i>		
<b>INITIATOR</b>		
Transient initiator with initial or subsequent MSIV closure	25	3
<b>SCRAM FUNCTION</b>		
RPS and manual scram failure	25	
<b>REACTOR PRESSURE VESSEL (RPV) WATER LEVEL CONTROL</b>		
Failure to control RPV water level at low pressure	25	
<b>AUTOMATIC DEPRESSURIZATION SYSTEM (ADS)</b>		
Failure to inhibit ADS (or prevent uncontrolled depressurization)	12	18
<b>HIGH PRESSURE INJECTION (HPCI/HPCS)</b>		
• Valves		
Steam inlet MOV (at turbine) fails to open	<1	
Injection line MOV near FW interface (HPCI) or RPV (HPCS) fails to open	<1	
Min flow valve fails to open	<1	
• Pump		
HPI pump fails to start or run	9	20
HPI pump unavailable due to test or maint.	4	20

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.

**Table 5.1 (Cont'd)**

*Sequence 6 (Cont'd.)*

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
• I&C		
Steam line drainpot level switch fails (no output)	<1	
System actuation train fails	<1	
Lube oil cooler loses flow	<1	

HPI total = 13

**DC POWER**

Loss of DC power from one station battery	<1	
-------------------------------------------	----	--

*BWR Representative Accident Sequence 7 - ATWS with Failure of SLC Injection*

**INITIATOR**

Transient initiator with failure to scram with or without PCS isolation	32	3
-------------------------------------------------------------------------	----	---

**SCRAM FUNCTION**

Failure of RPS and Manual Scram	32	
---------------------------------	----	--

**STANDBY LIQUID CONTROL (SLC) SYSTEM**

	<u>Enriched Boron</u>	<u>Two Pump Injection</u>	
• Human Error			
Operator fails to actuate system in time	21	10	28
System not restored (realigned) after testing	10	6	29
• Pumps			
SLC pump in test or maint.	1	3	
SLC pump(s) fail to start	<1	4	
• Valves			
SLC manual tank outlet valve (to pump suction) is plugged	<1	<1	
SLC relief valve fails to close diverting flow back to pump suction	<1	2	

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.

Table 5.1 (Cont'd)

Sequence 7 (cont'd)

<u>Event Description</u>	<u>Average Importance<sup>1,2</sup></u>	<u>Plant Specific Modifier Note</u>
Normally closed MOV at pump suction fails to open	<1	6
• Pipe Segments		
Failures in SLC pipe segment from explosive valves (EVs) to the RPV incl. EVs, check valves, sparger	1	2
SLC total = 33		

**REACTOR WATER CLEANUP (RWCU) SYSTEM**

RWCU isolation valve fails to close upon SLC actuation. Pentaborate is inadvertently removed from the RCS by RWCU	3	
-------------------------------------------------------------------------------------------------------------------	---	--

*BWR Representative Accident Sequence 8 - Unisolated LOCA Outside Containment*

**INITIATOR**

Large pressure boundary failure outside containment with failure to isolate	75	30
-----------------------------------------------------------------------------	----	----

**RECOVERY**

Mitigation of LOCA outside containment using the condensate system	25	
--------------------------------------------------------------------	----	--

<sup>1,2</sup> See General Notes 1 and 2 in the listing of Plant Specific Modifiers that accompanies this table.

## Plant Specific Modifier (PSM) Notes for Table 5.1

### General

1. The average importance is a composite of the four reference 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 general transient is composed of the following initiators:

Turbine trip (with subsequent MSIV closure)	(50%)
MSIV closure or loss of condenser vacuum	(30%)
Loss of main feedwater	(15%)
Inadvertently opened SRV (with MSIV closure)	(3%)
Loss of offsite power	(2%)
4. The loss of offsite power (LOOP) initiator is especially important at Millstone due to the limited high pressure injection and decay heat removal capability that remains available. Only FWCI and the IC are available at high RCS pressures and both are essentially single train systems. Multiply the average importance estimates for the LOOP initiator and offsite power recovery by a factor of 10 (sequences 1 and 2) for similar plant configurations.
5. Representative accident sequences 1 and 4 are losses of injection sequences. The failure of RPV makeup systems generally limits recovery measures to less than one hour.
6. The plant specific risk assessments that contribute to representative sequence 3 generally assume recovery measures must be successful before battery depletion or loss of reactor vessel makeup, which typically is expected to occur within six to eight hours of the SBO.
7. With the exception of IC makeup recovery (see note 9) a loss of decay heat removal provides in excess of fifteen hours for the recovery of key systems.
8. Primary containment venting is a containment preservation strategy of last resort and is usually considered in PRAs after RPV failure. However, for representative accident sequence 2 containment venting provides a decay heat removal mechanism to maintain reactor coolant injection and prevent core damage.
9. The isolation condenser makeup system must be recovered in approximately one hour to maintain IC operation.

### Emergency Power Systems

10. The failure of an emergency AC power source is important for HPCS or FWCI systems given a LOOP initiator. The average importance estimate should be multiplied by two for plants that have these systems.
11. The unavailability of an emergency AC (EAC) power source, subsequent to a LOOP, is generally important because it disables additional decay heat removal trains. This failure is especially important at Millstone because the shutdown cooling system has normally closed inlet and outlet MOVs that are powered by the opposite divisions. Thus, the failure of a single EAC source disables the SDC function. The average importance estimate should be multiplied by a factor of 2 for similar configurations.
12. Representative accident sequence 3 is a classical SBO that postulates a loss of the decay heat removal function due to a loss of AC power. The number of EDGs that must be unavailable to cause a station blackout can vary based on the design of the electrical distribution system. This is an especially important consideration at multi unit sites with shared EAC sources. For example, at Peach Bottom all four EDGs must be unavailable to have a SBO.
13. Representative accident sequence 4 is a short term failure of all RPV injection caused by a loss of AC power and unavailability of the DC powered sources of injection. The number of EDG failures is generally the same as sequence 3 with the possible exception of Grand Gulf where HPCS can fail due to component or EDG unavailability.
14. The average importance value is based on the loss of normal power logic that existed at Millstone during the development of the IREP. The logic contained two relays, either of which could fail and prevent all emergency loads from tying into the emergency power sources.
15. A major support system failure for shutdown cooling and containment cooling at Millstone is the loss of instrument AC power due to transformer/breaker malfunctions or bus transfer failure. At the time the IREP was being developed these components were not periodically tested and a failure would only be evident on demand. This resulted in a fairly high unavailability estimate for these components, and should be reflected by multiplying the average importance estimate by a factor of 3.
16. The common mode failure of all DC power is a major contributor to this sequence. The EDGs, HPCI, RCIC, the SRVs and the isolation condenser are dependent on DC power.

### Automatic Depressurization/Safety Relief Valves

17. Multiply the average importance value by a factor of two if the ADS initiation logic requires coincident high drywell and low RPV level signals or if ADS inhibit is procedurally required for scenarios like representative accident sequence 1.
18. The average importance estimate assumes an ADS inhibit switch is available in the control room. If the ADS timer must be continually reset to prevent uncontrolled depressurization multiply the average importance estimate by a factor of 2.

19. A stuck open relief valve can disable low capacity sources of high pressure injection such as the CRD hydraulic system. The SORV also eliminates the isolation condenser as a source of high pressure decay heat removal. Multiply the SORV average importance estimate by a factor of 3 for those plants with isolation condensers. Plants with HPCS/HPCI and RCIC systems should use an importance estimate of 1 (for sequence 2 only), as the decay heat removal systems at these plants are relatively unaffected by a SORV.

#### High Pressure Injection

20. The average importance estimates are based on the HPCI system. Within the context of sequences 1, 5, and 6 the HPCS system has a higher assessed availability. Multiply the average importance estimates by a factor of 0.2 (HPI pump failures) and 0.5 HPI test or maintenance unavailability.
21. The average importance estimate for representative sequence 4 is based on the HPCS system. Multiply by a factor of 3 to account for the higher unavailability of the HPCI turbine driven pump.
22. The CRD hydraulic system is credited in later BWR PRAs as a source of high pressure injection. System success usually requires two operating pumps and flow control station valve manipulations to maximize RPV flow.

#### Decay Heat Removal

23. The RHR system unavailability in sequence 2 is based on the prevalent BWR design that utilizes the same heat exchanger train for both containment heat removal and shutdown cooling. As such this design is susceptible to individual component failures. Some plants feature separate containment cooling and shutdown cooling systems.

For example, Millstone has two trains of LPCI/containment cooling supported by emergency service water (a standby system) and two trains of shutdown cooling which use the normally operating RBCCW/normal SW for cooling. This four train arrangement tends to be less vulnerable to individual component failures. The average importance estimates associated with individual component failures should be multiplied by a factor of 0.5 for this type of configuration.

24. The average importance value in sequence 2 is based on two RHR pumps, with dedicated suppression pool strainers. This estimate should be revised to <1 for configurations that are more redundant, i.e., the loss of a single strainer will not disable one train of RHR suppression pool (torus) cooling.
25. The isolation condenser (and its associated makeup system) is a single train system. The normally closed make-up valve<sup>1</sup> or mispositioned IC valves are AC powered by the gas turbine and would fail as-is in the event of an SBO.

---

<sup>1</sup> At Millstone, the IC makeup valve was changed to DC power after the IREP was completed.

### Service Water

26. The average importance estimate is based on a limited number of service water system pumps that are available to supply EDG cooling. For example, the Grand Gulf service water system is divided into separate trains for EDG cooling. Each train has only 1 SW pump. The unavailability of a single SW pump directly results in an EDG failure. In contrast, at Plant B, 2 out of 5 SW pumps are sufficient for all cooling loads, which makes random failures or maintenance unavailability of a single pump relatively unimportant. For similar SW system configurations revise the importance estimate to <1 for representative sequences 3 and 4.
27. The average importance estimate is based on a SW design that has normally closed valves in common portions of the supply or return from an EDG jacket water heat exchanger. The failure of a single valve therefore, disables EDG cooling. Revise the average importance estimate to <1 if all normally closed valves are arranged in parallel to avoid this concern.

### Standby Liquid Control

28. Under ATWS conditions, the BWROG EPGs require SLC initiation when the suppression pool temperature reaches approximately 105°F. This is generally estimated to occur in 2 to 7 minutes, depending on initial conditions and plant response.
29. Several SLC valves can fail system operation if they are not restored to their normal positions after testing. They are the normally closed manual valves in the return lines to the test and/or main tanks and any valves on the test or main tank outlet lines that are repositioned for testing.
30. Consists of the following failures:

Main steam lines	50
Feedwater	10
HPCI/RCIC lines	33
Interfacing LOCA <sup>1,2</sup>	7
(low pressure ECCS lines)	

<sup>1</sup> Where interfacing LOCA probability is defined as (initiating event probability) X (conditional failure probability to isolate the line) X (conditional failure probability of the low pressure system).

<sup>2</sup> Assumes on-line surveillance testing of injection valves is not permitted.

## 6. REFERENCES

1. NRC Maintenance Inspection Guidance, Volumes 1 and 2, September 1988.
2. U.S. NRC Inspection Manual, Chapter 2515, Temporary Instruction No. 2515/97, "Maintenance Inspection," Revision 1, September 22, 1989.
3. Travis, R., et al., "Generic Risk Insights for Westinghouse and Combustion Engineering Pressurized Water Reactors," US NRC Report NUREG/CR-5637, November 1990.
4. Kolaczowski, A.M., et al., "Analysis of Core Damage Frequency From Internal Events: Peach Bottom, Unit 2," US NRC Report NUREG/CR-4550, Vol. 4, October 1986.
5. U.S. NRC Inspection Manual, Chapter 2515, Procedure No. 93804, "Risk-Based Operational Safety and Performance Assessment," Revision 0, November 25, 1988.
6. Hester, O.V., et al., "Annotated Bibliography of Reliability and Risk Data Sources," U.S. NRC Report NUREG/CR-5050, March 1988.
7. Curry, J.J., et al., "Interim Reliability Evaluation Program: Analysis of the Millstone Point Unit 1 Nuclear Power Plant," U.S. NRC Report NUREG/CR-3085, February 1983.
8. Northeast Utilities, "Millstone Unit 1 Probabilistic Safety Study," July 1985.
9. Philadelphia Electric Co., "Probabilistic Risk Assessment Limerick Generating Station," March 1981.
10. Drouin, M.T., et al., "Analysis of Core Damage Frequency From Internal Events: Grand Gulf, Unit 1," US NRC Report NUREG/CR-4550, Vol. 6, April 1987.
11. 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.
12. Mirkovic, D., and Diamond, D.J., "Boron Flushing During a BWR Anticipated Transient Without Scram," U.S. NRC Report NUREG/CR-5573, June 1990.
13. Higgins, J.C., "Generic PRA-Based BWR Insights," BNL Technical Report A-3453-86, September 1986.



## APPENDIX A

### BWR 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 experience.

Table A-1 is derived from the representative accident sequences. Each "basic event" (i.e., component failure or human error) is listed including originating sequence(s), an importance estimate for ranking purposes and an inspection matrix that provides recommended 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:

$$I_l = \sum^R (I_l^{\wedge}(R) \cdot P(R))$$

where

$I_l$  = basic event importance estimate for event "l"

R = representative accident sequence number

$I_l^{\wedge}$  = average importance estimate for an event "l" of a representative accident sequence

P = Plant Specific Modifiers which revise the average importance estimate to incorporate risk significant plant specific design and operating features.

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. Sequences	Import. Est. 1,2	Inspection Matrix					Comments	
			Ops.	Surv.	Maint.	ISI/Test	Calib		Lic. Oper. Training/EOPs
<b>INITIATORS</b>									
Transients with immediate or subsequent loss of PCS	1, 2, 5, 6, 7		x	x	x		x	x	See PSM note 3, Table 5.1 for a description of this transient initiator.
Transient initiator with a subsequent loss of offsite power	3, 4		x	x	x		x	x	See PSM note 3, Table 5.1
Transient initiator with the main condenser available	7		x	x	x		x	x	See PSM note 3, Table 5.1
Loss of Offsite Power (LOOP) initiator	1, 2, 3, 4		x	x	x			x	See PSM notes 3 & 4, Table 5.1
Large pressure boundary failure outside containment with failure to isolate which typically includes the following failures:  Main steam lines      50% Feedwater lines      10% HPCL/RCIC lines      33% Interfacing LOCA*** 7% (low pressure ECCS lines)	8		x	x	x	x	x	x	
* Where interfacing LOCA probability is defined as (initiating event probability) X (conditional failure probability to isolate the line) X (conditional failure probability of the low pressure system).									
** Assumes on-line surveillance testing of injection valves is not permitted.									
Stuck Open Relief Valve (SORV)	1,2,4	(13)	x		x	x		x	See PSM note 19, Table 5.1

A-2

Notes: 1. See the general note, No. 1, in the Plant Specific Modifier (PSM) 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.  
 3. Importance estimates for the initiators can be qualitatively approximated using the sequence specific discussions in Section 4 and the qualitative sequence importance estimates of Table 4.1.

Table A.1 (Cont'd)

Event Description	Rep. Sequences	Import. Est. 1,2	Inspection Matrix						Comments	
			Ops.	Surv.	Maint.	ISI/Test	Calib	Lic. Oper. Training/EOPs		
<b><u>GENERAL RECOVERY ACTIONS</u></b>										
Failure to recover the power conversion system (PCS)	1,2	19	x						x	
Failure to recover offsite power	1,2,3,4	(2),(2),20,13	x						x	See PSM note 4, Table 5.1
Failure to successfully vent the containment	2	15	x						x	From a core damage perspective, containment venting failure is important only in loss of containment heat removal sequences. These sequences cause containment overpressure failure which can disable RPV injection and result in core damage.
Mitigation of a LOCA outside containment using the condensate system or ECCS with suction from the CST	8	25	x						x	
<b><u>EMERGENCY AC POWER</u></b>										
• Hardware Emergency generator (EG) fails to start or run (including common mode)	1,2,3,4	(2),(4),34,14		x	x			x		See PSM notes 10 & 11, Table 5.1
Breaker failure prevents loading the emergency generator	1,2,4	(2),(4),2		x	x					See PSM notes 10 & 11, Table 5.1
EG actuation logic failure	3,4	<1		x	x			x		
LOOP trip signal fails to reset, EGs unable to pick up load	4	(4)		x	x					See PSM note 14, Table 5.1
Emergency generator unavailable due to maintenance activities	3,4	5			x					
• Recovery Failure to recover from an emergency generator (EDG) hardware failure including common mode	3,4	13	x						x	

A-3

Notes: 1. See the general note, No. 1, in the Plant Specific Modifier (PSM) 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 (Cont'd)

Event Description	Rep. Sequences	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib	Lic. Oper. Training/EOPs	
Failure to recover from EG maintenance outage • Instrument/Control Power	3,4	2	x		x			x	
Transformer/breaker malfunction disables instrument power and pump cooling for the RHR containment and shutdown cooling modes	2	(5)		x	x				See PSM note 15, Table 5.1
Instrument power automatic bus transfer fails disabling instrument power, and pump cooling for the RHR containment and shutdown cooling modes	2	(3)		x	x				See PSM note 15, Table 5.1
<u>DC POWER</u>									
Battery failure (including common mode)	3,4,5,6	18		x	x				
Battery charger failure	3	<1		x	x		x		
DC battery/bus unavailable due to maintenance activities	4	<1			x				
Recovery									
Failure to recover from a battery fault	4	1	x					x	
<u>HIGH PRESSURE INJECTION (HPI)</u> <u>HPCI/HPCS/FWCI</u>									
• Hardware Valves									
HPI min flow valve fails to open (including controller faults)	4,5,6	2		x	x	x	x		
HPI injection line valve(s) failure	4,5,6	2		x	x	x			
Condensate storage tank outlet valve plugged	4	<1		x	x				
Steam inlet valve (at turbine) fails to open	5,6	<1		x	x	x			

Notes: 1. See the general note, No. 1, in the Plant Specific Modifier (PSM) 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.

A-4

Table A.1 (Cont'd)

Event Description	Rep. Sequences	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib	Lic. Oper. Training/EOPs	
Turbine/pump HPI pump fails to start or run	1,4,5,6	(8),(1),(14),(9)		x	x	x			See PSM notes 20 & 21, Table 5.1
Failure of pump breaker	1	1		x	x				
Lube oil cooler hardware failure	5	<<1		x	x	x			
Loss of cooling water flow to lube oil cooler	6	<1		x	x	x			
• I&C									
HPI actuation logic failure	1,4,5,6	1		x	x		x		See PSM note 20, Table 5.1
Suppression pool switchover logic fails	5,6	1		x	x		x		
Level switch at steam line drain pot fails	5,6	1		x	x		x		
HPI system unavailable due to test or maintenance activities (primarily pump and/or turbine)	1,4,5,6	(2),<1,(6),(4)		x	x				
Failure of pump pressure permissive switch (FWCI)	1	<1		x	x		x		
Pump pressure permissive switch unavailable due to test or maintenance	1	<1		x	x				
RCIC									
• Operator Error									
Operator fails to manually start RCIC given auto actuation failure	4	<<1	x					x	
• Hardware Valves									
Min flow valve fails to open (including controller failures)	4	<1		x	x	x	x		
Steam inlet valve (at turbine) fails to open	4	<1		x	x	x			

Notes: 1. See the general note, No. 1, in the Plant Specific Modifier (PSM) 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.

A-5

Table A.1 (Cont'd)

Event Description	Rep. Sequences	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib	Lic. Oper. Training/EOPs	
Steam line containment isolation valve fails to open	4	<1		x	x	x			
Injection line valve (near FW/RCIC interface) fails to open	4	<1		x	x	x			
<b>Turbine/Pump</b>									
RCIC turbine driven pump (TDP) fails to run	1,4	6		x	x	x			
RCIC lube oil cooler hardware failure	4	<1		x	x	x			
<b>General</b>									
RCIC system unavailable due to test or maintenance activities (primarily TDP)	1,4	3		x	x				
<b>• I&amp;C</b>									
RCIC actuation logic fails	4	<1		x	x		x		
<b>CONTROL ROD DRIVE HYDRAULIC (CRDH) SYSTEM</b>									See PSM note 22, Table 5.1
<b>• Human Error</b>									
Operator fails to manually start and align the second CRD pump	1	2	x					x	
Operator fails to align CRDH system valves to maximize RPV injection	1	1	x					x	
<b>• Hardware Pumps</b>									
CRD pump fails to start	1	<1		x	x				
CRD pump unavailable due to maintenance activities	1	<1			x				

Notes: 1. See the general note, No. 1, in the Plant Specific Modifier (PSM) 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 (Cont'd)

Event Description	Rep. Sequences	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib	Lic. Oper. Training/EOPs	
<b><u>AUTOMATIC (ADS)MANUAL DEPRESSURIZATION</u></b>									
● Human Error									
Failure to manually depressurize using non-ADS valves	1	(10)	x					x	See PSM note 17, Table 5.1
Failure to inhibit ADS (or prevent uncontrolled depressurization) during ATWS	6	(12)	x					x	See PSM note 18, Table 5.1
● Hardware									
ADS valve fails to open including ADS common mode failure to O-ring leakage	1	12		x	x	x			
<b><u>SERVICE WATER (SW) SYSTEM</u></b>									
● Human Error									
Operator fails to start SW booster pump to provide EDG cooling	3,4	3	x					x	
● Hardware Valves									
Common mode failure of SW valves disables flow to both RHR heat exchangers	2	<1		x	x	x			
SW common inlet or return valve to EDG jacket HX in maintenance	3	<1			x				
Pumps									
SW pump fails to run	2,3,4	(10),(3),(1)		x	x	x	x		See PSM notes 23 & 26, Table 5.1
SW pump unavailable due to maintenance activities	3,4	(1)			x				See PSM note 26, Table 5.1

A-7

Notes: 1. See the general note, No. 1, in the Plant Specific Modifier (PSM) 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 (Cont'd)

8-V

Event Description	Rep. Sequences	Import. Est. 1,2	Inspection Matrix						Comments
			Ops.	Surv.	Maint.	ISI/Test	Calib	Lic. Oper. Training/EOPs	
<b>Heat Exchangers (HX)</b>									
RHR HX fails due to plugging on the SW side	2	(2)		x	x				See PSM note 23, Table 5.1
RHR HX unavailable due to SW test or maintenance activities	2	(5)		x	x	x			See PSM note 23, Table 5.1
<b>General</b>									
SW emergency diesel generator (EDG) jacket cooling HX train fails (primarily HX inlet or outlet valves)	3,4	(6)		x	x	x			See PSM note 27, Table 5.1
SW EDG HX train (primarily jacket cooler HX) out for maintenance	3	<1			x				
Mechanical SW failure prevents FWCI pump cooling	1	1		x	x	x			
Common mode failure of SW trains fails all EDG cooling	3	<1		x	x	x	x		
<b><u>RESIDUAL HEAT REMOVAL (RHR) SYSTEM</u></b>									
● <b>Hardware</b>									
<b>Valves</b>									
Min flow valve fails to open on demand including common mode	2	(1)		x	x	x	x		See PSM note 23, Table 5.1
Heat exchanger bypass valve fails to close, including common mode	2	(1)		x	x	x			See PSM note 23, Table 5.1
Suppression pool return valve fails to open, including common mode	2	(1)		x	x	x			See PSM note 23, Table 5.1
Plugging of RHR suppression pool strainer	2	(1)		x	x				See PSM note 24, Table 5.1
● <b>Recovery</b>									
Failure to recover RHR failed valve	2	(3)	x					x	See PSM note 23, Table 5.1

Notes: 1. See the general note, No. 1, in the Plant Specific Modifier (PSM) 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 (Cont'd)

Event Description	Rep. Sequences	Import. Est. 1,2	Inspection Matrix					Comments	
			Ops.	Surv.	Maint.	ISI/Test	Calib		Lic. Oper. Training/EOPs
RHR loop unavailable due to testing or maintenance activities	2	(1)		x	x	x			See PSM note 23, Table 5.1
<u>ISOLATION CONDENSER (IC) AND MAKEUP SYSTEM</u>									See PSM note 25, Table 5.1
● Human Error									
IC isolation valves not restored to correct position after test or maintenance	4	1	x	x	x	x			
● Hardware									
IC makeup valve fails to open	1	2		x	x	x			
IC isolation valves closed due to test or maintenance activities	1	2			x	x			
IC initiation logic relay contacts fail to operate	1	1		x	x	x			
● Recovery									
Failure to recover IC makeup by manually opening valve	1,2,4	7	x					x	
<u>Condensate Transfer System</u>									
Failure of the condensate transfer system to provide makeup to the FWCI system	1	1		x	x	x			
<u>Room Cooling (HVAC)</u>									
● Recovery									
Failure to recover switchgear or battery room cooling	1,4	5	x					x	
● Hardware									
Switchgear or battery room cooling fails disabling a bus	1,3,4	8		x	x				

A-9

Notes: 1. See the general note, No. 1, in the Plant Specific Modifier (PSM) 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 (Cont'd)

Event Description	Rep. Sequences	Import. Est. 1,2		Inspection Matrix					Comments	
				Ops.	Surv.	Maint.	ISI/Test	Calib		Lic. Oper. Training/EOPs
Emergency generator (EG) room cooling fails including fan and damper failures	3,4	1			x	x				
EG room HVAC unavailable due to maintenance	3,4	<1				x				
Switchgear or battery room HVAC out for maintenance	3,4	2				x				
<u>STANDBY LIQUID CONTROL (SLC) SYSTEM</u>		Enriched Boron	Two Pump							
● Human Error										
Operator fails to manually actuate system in time	7	21	10	x					x	See PSM note 28, Table 5.1
System not restored (realigned) after testing	7	10	6	x	x		x		x	See PSM note 29, Table 5.1
● Hardware Valves										
SLC relief valve fails to close, diverting flow back to the pump suction	7	<1	2		x	x	x	x		
SLC manual tank outlet valve (to pump suction) is plugged	7	<1	<1		x	x				
Normally closed MOV at pump suction fails to open	7	<1	6							
Pumps										
SLC pump(s) fail to start	7	<1	4		x	x				
SLC pump unavailable due to test or maintenance activities	7	1	3		x	x	x			

A-10

Notes: 1. See the general note, No. 1, in the Plant Specific Modifier (PSM) 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 (Cont'd)

Event Description	Rep. Sequences	Import. Est. 1,2	Inspection Matrix					Comments	
			Ops.	Surv.	Maint.	ISI/Test	Calib		Lic. Oper. Training/EOPs
Pipe Segment									
Failure in SLC pipe segment from the explosive valves (EVs) to the RPV prevents flow (includes the EVs, check valves, and sparger)	7	1 2		x	x	x			
<u>SCRAM FUNCTION</u> Failure of the reactor protection system (RPS) and failure to successfully manually scram	5,6,7	82	x	x	x		x	x	
<u>REACTOR WATER CLEANUP (RWCU) SYSTEM</u> RWCU isolation valve fails to close upon SLC actuation. Pentaborate is inadvertently removed from the reactor coolant	7	3		x	x	x			
<u>RPV WATER LEVEL CONTROL (POST ATWS)</u> Operator fails to manually depressurize RPV (given HPCI/HPCS failure, ADS inhibited). The remaining high pressure systems cannot keep the core covered	5	25	x					x	
Failure to control RPV water level at low pressure i.e., failure to inhibit ADS (or otherwise control RPV depressurization) and/or failure to prevent uncontrolled low pressure injection	6	25	x					x	
<u>RPV LEVEL INSTRUMENTATION</u> Common mode miscalibration	4	<<1		x			x		

A-11

Notes: 1. See the general note, No. 1, in the Plant Specific Modifier (PSM) 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 PRA 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. 5), 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 the time limitations for the successful recovery of critical functions? A loss of decay heat removal sequence (i.e., representative sequence 2) can allow upwards of fifteen hours for recovery of offsite power or the PCS. In contrast, loss of injection sequences typically require recovery in less than one hour to prevent core damage. A rough idea of the available recovery time is essential for prioritizing plant response.
- Is there a reasonable assurance of system/component operability under accident conditions? For example, does the plant have a program for the periodic bench testing and refurbishing of the safety relief valves? PRAs generally assign a high hardware reliability for automatic and manual depressurization, as well as valve reclosure after actuation. Is this assumption supported by the testing results?
- Do degraded plant conditions permit access to remotely operated equipment? Are recovery actions feasible? The secondary containment environment associated with station blackout or containment venting can limit manual recovery actions.

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 GE BWRs. Table A.1 is an inspection matrix that combines the failures of the eight 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 Susquehanna and the Mark I BWR applications (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 Section 4 (Table 4.1) and plant specific design and operating information
  - If no information is available, leave sequence ranking as highly important
  - 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 Section 5 (Table 5.1) and detailed plant specific information
  
4. **Develop Simulations for the Selected Sequences**
  - Use the accident sequence descriptions of Section 4 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:

- Will MOV closure occur under interfacing system LOCA conditions?
- 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) based on:
    - 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<sup>1</sup>**

---

P&ID drawings  
System Descriptions or training manuals  
Technical Specifications  
FSAR sections

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

Records of system modifications  
Records of system maintenance, testing

---

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