NUREG/CR-6432
SEASF-DR-94-001

Estimated Net Value and Uncertainty for Automating ECCS Switchover at PWRs

Manuscript Completed: January 1996
Date Published: February 1996

Prepared by
B. Walsh, J. Brideau, L. Comes, J. Darby, H. Guttmann, F. Sciacca,
F. Souto, W. Thomas, G. Zigler

Science and Engineering Associates, Inc.
6100 Uptown Boulevard, NE
Albuquerque, NM 87110

J. Jackson, NRC Project Manager

Prepared for
Division of Engineering Technology
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC Job Code W6325

ABSTRACT

A central question for resolution of GSI-24 is whether or not PWRs that currently rely on a manual system for ECCS switchover to recirculation should be required to install an automatic system. Risk estimates are obtained by reevaluating the contributions to core damage frequencies (CDFs) associated with failures of manual and semiautomatic switchover at a representative PWR. This study considers each separate instruction of the corresponding emergency operating procedures (EOPs), the mechanism for each control, and the relationship of each control to its neighbors. Important contributions to CDF include human errors that result in completely coupled failure of both trains and failure to enter the required EOP.

This detailed study finds that changeover to a semiautomatic system is not justified on the basis of cost-benefit analysis: going from a manual to a semiautomatic system reduces the CDF by 1.7×10^{-5} per reactor-year, but the probability that the net cost associated with the modification being less than $1,000 per person-rem is about 20% without license renewal. Scoping analyses, using optimistic assumptions, were performed for a changeover to a semiautomatic system with automatic actuation and to a fully automatic system; in these cases the probability of having a net cost being less than $1,000/person-rem is about 50% without license renewal and over 95% with license renewal.

Table of Contents

List of Tables

List of Figures

1.0 Introduction

1.1 Objectives

This report documents results from Task 4 of Contract NRC-04-91-071. Task 4 provides technical assistance to the Nuclear Regulatory Commission (NRC) staff in the evaluation and resolution of Generic Safety Issue No. 24 (GSI-24), "Automatic ECCS Switchover to Recirculation."

Current NRC review criteria (NRC, NUREG-0800) state that an automatic system is preferable for switchover of the Emergency Core Cooling System (ECCS), but that a manual system is acceptable if it meets certain conditions. The central question for resolution of GSI-24 is whether or not licensees of pressurized water reactors (PWRs) that currently rely on a manual switchover system should be required to install an automatic system.

The objective of the work described in this report was to develop a technical findings document which would

- estimate the core damage frequency (CDF) and risk changes (and uncertainty) that would result from changeover to an automatic switchover system,
- estimate what it would cost (with uncertainty) for a licensee to install such an automatic switchover system, and
- perform a probabilistic cost-benefit analysis of the risk and cost information.

The risk estimates were obtained by reevaluating the risks associated with failures of manual and automatic switch-over at a representative PWR. The representative automatic system, selected in consultation with the NRC Task Manager, is considered to be a "semiautomatic" system and is based on a modification that had been designed and implemented at a Westinghouse PWR. It was selected in part because the modification was performed at only one of two units at the same site, permitting a direct comparison of control room layouts and emergency operating procedures before and after the modification.

The information developed to complete this task was also used to draw inferences regarding the potential benefits of other alternatives, including changeover to a fully automatic system.

1.2 Organization of This Report

The next section of this report explains the primary safety issues associated with GSI-24, including the significance of the ECCS switchover process, some of the applicable history of regulatory activity, and potential alternative backfits to existing manual systems.

Section 3 presents the method for calculating CDF and risk estimates for the representative systems. The method used linking of the failure model for the switchover system at the representative plant to an existing Probabilistic Risk Assessment (PRA) model for a similar PWR.

Section 4 presents the design of a representative semiautomatic switchover system. Section 5 presents the failure logic models for a manual and a semiautomatic system at the representative PWR, and Section 6 contains the reliability analysis of the human errors and automatic control failures included in the model. The bulk of Section 6 is devoted to a detailed human reliability analysis of the relevant operating procedures.

The calculated contributions of manual and semiautomatic switchover control failures to the CDF of the representative plant appears in Section 7, together with estimates of uncertainty.

Section 8 discusses the consequences of a core damage event that might result from failure of ECCS switchover. Estimates are presented for three types of containment, with attention to the conditional probability of containment failure and the public dose within 50 miles.

Section 9 provides the rationale for the selection of alternative backfits to be included in cost-benefit studies and provides the general assumptions made in those studies. Sections 10 and 11 report two cost-benefit analyses, the first for changeover to the semiautomatic system and the second for backfitting to a single failure criterion for certain manual operations. Inferences are drawn regarding the potential net value of further automation. Section 12 summarizes the findings of this study.

The appendices contain additional explanatory or supporting material. They include a more elementary explanation of the role of ECCS switchover, current standards for switchover control, a survey of the current status of switchover automation at operating PWRs, and discussions of methodologies for human reliability analyses.

2.0 Generic Safety Issue No. 24

2.1 ECCS Switchover to Recirculation

This section surveys the reactor systems and functions that were the subject of this study, establishes the issues that are addressed, reviews key aspects of the methodology, and notes the terminology that was used in this report. The reader who is not familiar with these systems should refer to the more detailed discussion in Appendix A.

A PWR generates heat in a core that is cooled and moderated by light water. Heat is transferred from the reactor core by the Reactor Coolant System (RCS), which circulates through high-pressure loops. To maintain the chemical content and volume of the RCS coolant inventory, charging (CHG) pumps inject coolant into the high-pressure RCS loops. During power operation, heat is removed by boiling water in the steam generators. The main turbine generators extract power from the steam to generate electricity.

After a normal interruption of power operation, initial shutdown cooling is accomplished by using the main turbine bypass system to direct steam to the main condensers. After initial cooldown and depressurization, the Residual Heat Removal (RHR) System directs reactor coolant to the RHR heat exchangers.

Loss-of-coolant accidents (LOCAs) are accidents that would result if the rate of loss of reactor coolant exceeded the capability of the reactor coolant makeup system. The ECCS first injects makeup water into the RCS during a LOCA and later recirculates water through the core following a LOCA to provide for long-term post-accident core cooling. In all PWRs, the ECCS includes high- and low-pressure safety injection (HPSI and LPSI) pumps. In most PWRs, the RHR pumps perform the LPSI function. At many plants the HPSI function is performed in whole or in part by the normal charging pumps.

During the injection phase of operation following a large LOCA, the RCS is rapidly depressurized. Both the HPSI and LPSI pumps are aligned to take suction on the Refueling Water Storage Tank (RWST) and deliver makeup water to the reactor vessel. Water lost from the RCS is collected in the containment sump. The coolant injection and heat transport paths associated with large LOCA mitigation are shown in Figure 2.1, taken from the Nuclear Power Plant System Sourcebook (NRC, NUREG/CR-5640). Following a small LOCA, the RCS may slowly depressurize or remain at or near normal operating pressure, preventing injection by LPSI pumps.

When the RWST makeup water supply reaches a low level, the ECCS is placed in the recirculation mode of operation by aligning the suctions of the LPSI pumps to the containment sump and isolating the suction path from the RWST. In most PWR plants, the HPSI pumps cannot be aligned to take a suction directly from the containment sump. At the time recirculation is actuated, the normally dry containment sump is full of water that has collected from the RCS break and from the operation of the containment spray system. The break has contributed water that was in the RCS at the time of the accident and additional water from ECCS operation. During recirculation, water returns to the containment sump through the RCS break that caused the LOCA.

Following a large LOCA, the RCS is depressurized to the point that the LPSI pumps can provide continuous makeup to the RCS, and the HPSI pumps may be stopped. Heat exchangers in the LPSI system may be used during the recirculation phase to transfer heat to the ultimate heat sink. The low-pressure ECCS recirculation loop is comparable to the RHR shutdown cooling loop with the exception that the low-pressure pumps are aligned to take suction from the containment sump.

During a small LOCA, RCS pressure may remain high at the time that the RWST reaches the switchover level (i.e., when pump suction must be switched from the RWST), precluding recirculation with just the LPSI pumps. In this case, 2-loop Combustion Engineering PWRs can be aligned such that the HPSI pumps take a suction on the containment sump, but most other plants establish the high-pressure recirculation flow path with the LPSI and HPSI pumps operating in tandem. In tandem operation the low-pressure pumps take a suction on the containment sump and are aligned to deliver the water to the suction of the high-pressure pumps, which then inject water into the RCS. Heat

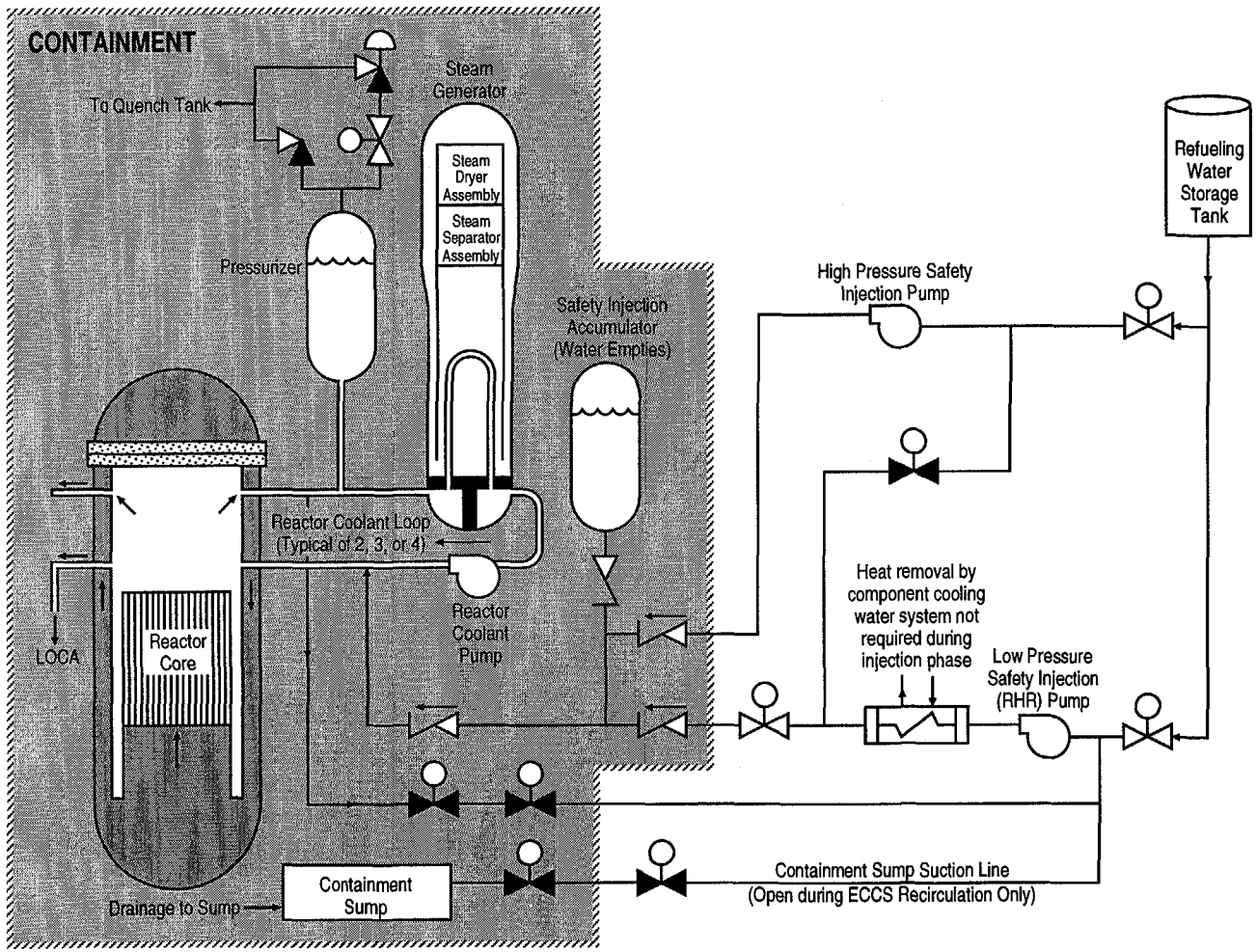

Figure 2.1 ECCS Injection and Heat Transport Paths During a Large LOCA

exchangers in the LPSI system may be used during high-pressure recirculation to transfer heat to the ultimate heat sink.

The switchover functions that may be considered for automation are:

- Realignment of the LPSI pumps suction
- Realignment of the HPSI pumps suction
- Actuation

Each realignment step requires the realignment of several valves.

A switchover system is usually considered to be "automatic" if both LPSI and HPSI alignment are automated, even if actuation is manual. A "semiautomatic" system is one that performs the LPSI realignment process, but leaves HPSI realignment for the operator.

An automated system normally contains logic that can inhibit the switchover under specified conditions, such as the RWST level not being low. For example, at the representative plant considered in this study, LPSI realignment can be sequenced automatically, but the logic requires RWST level low, sump level high, and switchover enabled.

Whether actuation is automatic or manual may depend on the plant's Emergency Operating Procedure (EOP). For example, at the representative plant actuation is manual because the EOP requires that the operator independently verify that the RWST and sump levels are appropriate before enabling switchover.

2.2 Generic Issue No. 24

GSI-24 addresses post-LOCA ECCS switchover to recirculation in PWRs that are currently operating. The overall issue is whether there is supportable preference among, or need for modification to, manual, semiautomatic, or automatic systems. "Supportable" is in the context of the backfit rule and relevant cost/benefit guidance.

Appendix B describes current acceptance criteria for ECCS switchover systems. In particular, ICSB 20 considers ECCS switchover acceptance criteria in comparison with the requirements for protection system actuation (NRC, NUREG-0800). Automatic transfer to the recirculation mode is stated to be preferable. A design that provides manual actuation at the system level, while not ideal, is considered to be sufficient provided that

- adequate instrumentation and information display are available to the operator so that he can make the correct decision at the correct time and
- in case of operator error, there are sufficient time and information available so that the operator can correct the error with acceptable consequences.

Appendix C contains information on the status of ECCS switchover control at each operating U.S. PWR. The aspect of GSI-24 that is addressed in this report concerns whether plants with manual systems should be required to automate them. The resolution of this issue for a particular plant may depend on the reliability of the manual system. Therefore the quality of displays, EOPs, and training are associated issues.

2.3 The Role of PRA

A Level 1 PRA consists of an analysis of plant design and operation focusing on accident sequences that could lead to core damage, their basic causes, and frequencies. The results include a long list of the various combinations of basic failure events that can lead to core damage. Examples of basic failure events are a specific pump failing to start, two valves failing to close from an unknown common cause, an operator failing to take a specific corrective action, or a specific unit being unavailable because of scheduled maintenance. Each combination of basic events that would cause core damage is called a cut set.

Two kinds of accident initiators are considered for a Level 1 PRA, initiating events that occur within the power plant systems themselves and accident initiators caused by events external to the power plant systems. Examples of external initiators include earthquakes, floods, and high winds.

The results of a Level 1 PRA provide assessments of plant safety, design and procedural adequacy, and

insights into how the plant functions from the perspective of preventing core damage. In particular, by identifying those cut sets which contain a particular event, the analyst can determine the portion of CDF that involves that failure event, called the contribution of the event to CDF.

The contribution to CDF is a measure of the sensitivity of total risk to changes in the probability of that basic event. The CDF can have a sensitivity to various changes, for example

- replacing a probability based on industry data with a value based on plant data,
- degradation or ineffective maintenance that causes the probability to increase, or
- investments in engineering or training that result in improved performance.

Similarly, the contribution of a particular system, component or operation, to CDF can be evaluated by identifying all cut sets that contain one or more failures related to that particular system, component or operation. Such information can provide guidance as to whether further study of an issue is warranted.

2.4 Reported Contribution of ECCS Switchover to Plant Risk

Four published PRAs for internal events were found to include sufficient information to approximate the contribution to CDF from failure to transition to recirculation. One is the NSAC PRA for Oconee Unit 3 (Nuclear Safety Analysis Center). Another is the Sandia National Laboratories (SNL) Level 1 internal events PRA for Sequoyah Unit 1 (Bertucio and Brown), which was part of a five-plant study of severe accident risks (NRC, NUREG-1150). The remaining two PRAs are the licensee submittals for H. B. Robinson (Carolina Power & Light Company) and Haddam Neck (Northeast Utilities Service Company) under the Individual Plant Examination (IPE) program. The information is presented in Table 2.1.

2.4.1 Oconee

The Oconee switchover system is fully manual. In the NSAC analysis, LOCAs were calculated to contribute a CDF of 1.6×10^{-5} per reactor-yr, with 9.2×10^{-6} being contributed by failures of operations staff to decide on and correctly implement switchover.

In the NSAC PRA for Oconee, failure to decide on and implement low pressure recirculation was modeled as a basic failure event, with a comparable event for high-pressure recirculation. The estimated failure probability for low-pressure switchover control is 5.0×10^{-3} per demand, assuming approximately 30 minutes are available after the LOCA, leading to a CDF contribution of 4.7×10^{-6} per reactor-yr. Failure to complete high-pressure switchover within two hours after the initiating event was given a probability of 3.0×10^{-3} per demand and contributes 4.5×10^{-6} per reactor-yr.

2.4.2 Haddam Neck

At Haddam Neck, manual actions would be required to accomplish ECCS switchover. This plant has distinct LPSI and RHR pumps, with the RHR pumps required to recirculate from the ECCS sump.

The point-estimate CDF contribution from internally initiated events was 1.8×10^{-4} per reactor-yr. LOCA scenarios were found to represent almost 32% of the total CDF. The dominant contributor to the LOCA sequences was determined to be the failure of operators to transfer to sump recirculation after a medium or large LOCA. As discussed in the Haddam Neck IPE submittal, approximately 16% of the CDF, or about 50% of the LOCA accident sequence frequency, was attributed to this operator failure. There is a very short time available for the operators to accomplish the transfer procedure because of relatively low RWST capability (100,000 gallons), large pumping capacity of the LPSI pumps, and a large number of operator actions needed to perform the switchover. Note that RWSTs at later vintage PWRs contain on the order of 300,000 gallons. Based on the above data, it was estimated that the contribution to the CDF from failure to manually establish recirculation is 16% of 1.8×10^{-4}, or 2.9×10^{-5}, per reactor-yr.

Table 2.1 Reported CDF Contributions From Failure of ECCS Switchover

Site	CDF contribution (10^{-5}/reactor-yr) PRA	LOCAs	Switchover	Type
Oconee	NSAC	1.6	0.9	Manual
Sequoyah	NUREG-1150	3.6	2.7	Semiautomatic
Robinson	IPE	8.	4.5	Manual
Haddam Neck	IPE	5.8	2.9	Manual

Finally, the IPE submittal summarizes human error probabilities for the failure to transfer to sump recirculation. These errors are divided into two portions, specifically cognitive and manipulative actions. The failure probabilities used in the analyses are listed below.

Small LOCA cognitive = 0.002
manipulative = 0.001

Medium LOCA cognitive = 0.013
manipulative = 0.003

Large LOCA cognitive = 0.05
manipulative = 0.01

2.4.3 H. B. Robinson

H. B. Robinson is a Westinghouse 3-loop PWR that first achieved commercial operation in 1971. At this plant, manual actions are required to achieve ECCS switchover. Robinson has a large dry containment. The total CDF was estimated to be 3.2×10^{-4} per reactor-yr. This estimate included internally-generated flooding scenarios. Of this total CDF, LOCA initiators contributed 23%, interfacing system LOCAs contributed 1%, and transient-induced LOCAs contributed 21%. Note that the RWST used at Robinson has a minimum capability of 300,000 gallons during plant operations.

The following results were extracted from the IPE submittal:

a) 11% of the CDF was associated with a medium LOCA and failure to successfully establish recirculation; the dominant contributor is the failure of operations staff action involved in performing switchover alignment;

b) 3% of the CDF was associated with a large LOCA and failure to successfully establish recirculation; the dominant contributor is failure of the operations staff action to perform lineup from the low head safety injection discharge to the high head safety injection suction line.

The submittal does not list individual event contributors to CDF. However, an upper bound for the fractional contribution of manual switchover failure to the CDF can be estimated as 0.11+0.03=0.14. In other words, the failure to manually establish recirculation could represent a contribution of as much as 4.5×10^{-5} per reactor-yr to the CDF.

Finally, mean probabilities of events used to model operator failure to achieve switchover are listed below. These values were extracted from the IPE submittal.

20 minute time frame:
Small LOCA 0.0038
Medium LOCA 0.0066
Large LOCA 0.012
Trans w/Flood 0.0095

40 minute time frame:

Medium LOCA	0.0029
Large LOCA	0.0072

2.4.4 Sequoyah

Sequoyah, on the other hand, has a semiautomatic ECCS switchover system. The NUREG-1150 analysis calculated a CDF of 3.6×10^{-5} per reactor-yr from LOCAs. Switchover control failures contributed at least 2.7×10^{-5} per reactor-yr (Bertucio and Brown).

The reason that the NUREG-1150 analysis estimated a comparable contribution to the LOCA CDF, in spite of the presence of a semiautomatic switchover system, is that SNL analysis divided the switchover process into its separate functions, identifying failure modes that had not been considered in the other PRAs.

The NUREG-1150 Sequoyah PRA treated failures of the actuation system to generate low-pressure switchover
signals for Train A and Train B as two basic failure events, each with failure probability of 1.6×10^{-3} per demand and no significant contribution to CDF. The only other basic event for low-pressure switchover control is miscalibration of the RWST level sensors, which was estimated to have an unavailability of 5.0×10^{-4}. This type of miscalibration would fail both ECCS trains and contributed 2.8×10^{-6} per reactor-yr to the CDF.

This Sequoyah PRA modeled manual operations for high-pressure switchover at the level of individual valves. Three of these valve operation errors, all with probabilities between 2.0×10^{-3} and 3.0×10^{-3} per demand, were found to be top contributors to CDF; their total contribution was 2.4×10^{-5} per reactor-yr. These operator errors were modeled as coupled failures: when the error was made for one train, it was assumed that the same error was made for the other train.

2.4.5 Switchover Failure Probabilities

The IPEs submitted by several other licensees were surveyed for data regarding the failure probability for manual ECCS switchover (Commonwealth Edison, Duke Power Company, Florida Power & Light, Wisconsin Electric Power Company, and Wisconsin Public Service Corporation). All of them listed a value in the Human Reliability Analysis (HRA) data for failure to switchover to recirculation mode, although some gave different values for different initiators. These are listed in Table 2.2 together with the values from the IPEs discussed earlier in this section. It appears that the models included the failure of manual ECCS switchover as a single, lumped event. The failure probability used in the Oconee IPE is much less than the values used in the NSAC analysis of Oconee.

Table 2.2 Manual Switchover Failure Probabilities Used in IPE Submittals

Plant	Large LOCA	Medium LOCA	Small LOCA
Haddam Neck	0.06	0.016	0.003
Kewaunee	0.00035 (align 1 train) 0.000049 (align 1 of 2 trains)		
Oconee	0.001	0.001	0.001
Point Beach	0.1	0.0097	0.0097
Robinson	0.012	0.0066	0.0038
Turkey Point	0.12	0.03	0.0078
Zion	0.0022 (with sprays) 0.00043 (all other cases)		

2.5 Requirement for Continuous Flow

At some plants with manual switchover, the EOP specifies that the LPSI pumps be stopped during the switchover and then restarted. This situation has at least the following disadvantages:

(1) The time required to stop and restart the pumps leaves less time to complete the remaining switchover operations.

(2) The pumps must be restarted soon enough that the ECCS continues to satisfy the criteria for successful cooling.

(3) Stopping the pumps exposes the switchover procedure to the additional risk that one or more pumps fail to restart on demand, including a common-cause failure of all pumps to restart.

At least two plants have modified EOPs to reduce the time allowed for interruption of ECCS during low-pressure switchover. At one plant, the EOP had required all safety injection pumps to be stopped simultaneously during switchover and had allowed up to ten minutes to perform the switchover. Subsequent analysis, taking into account large-scale LOCA simulation tests, indicated that interruption of only about two minutes after a large break LOCA may result in core uncovery. The utility revised the EOPs to ensure proper flow during switchover (Hodges).

Another plant had permitted an interruption in safety injection flow for as long as three minutes following a large break LOCA and ten minutes following a small break LOCA. Revised procedures ensure that no interruption of ECCS flow to the vessel occurs following a large break LOCA, and only a three-minute period of interruption occurs for the small break LOCA (Westinghouse Electric Corporation).

At a third plant, the switchover was performed one train at a time, but there was no procedure to cope with the event of a single failure leading to one inoperable safety injection train. Therefore, in the event of a single failure, the ECCS injection might have been interrupted for more than two minutes, resulting in core uncovery. As a result of this review, the utility committed to re-evaluate and modify their EOPs to satisfy the single failure criterion (Hodges).

2.6 Potential Alternative Approaches

To proceed with this study it was necessary to select potential approaches to reducing risk associated with existing manual and semiautomatic ECCS switchover control systems. As a result of the considerations discussed in the preceding sections, the following suggested themselves as potential alternatives:

- Requiring that EOPs be modified as necessary to assure that switchover can be accomplished assuming one operator error in valve or pump operations (manual and semiautomatic systems),
- Requiring modification to eliminate stopping and restarting the pumps (manual systems only),
- Requiring that valve operations for low-pressure switchover be sequenced automatically once actuated (conversion to semiautomatic, applicable to manual systems only),
- Requiring that valve operations for low-pressure switchover be actuated and sequenced automatically (manual and semiautomatic systems),
- Requiring that valve operations for low-pressure and high-pressure switchover be actuated and sequenced automatically (conversion to fully automatic, applicable to manual and semiautomatic systems).

2.7 Uncertainty Distributions

This report includes a comparison of some potential alternatives, including evaluations that would be necessary for a regulatory analysis. A regulatory analysis should discuss the magnitudes of uncertainties in estimates. Formal uncertainty analysis typically requires computer calculations.

Where the value of a parameter is uncertain, the best estimate is the mean of all possible values, weighted by their relative likelihood. Formal uncertainty analysis requires that each best estimate be supplanted by a cumulative probability distribution for the possible values of the parameter. This "uncertainty distribution" indicates, for various possible values of the parameter, the probability that the actual value will not be greater. This could be expressed, for example, as a table of percentiles for that parameter. The 5th percentile and the 95th percentile would be low and high estimates; the actual value should fall between them 90% of the time. The 50th percentile would be the median; in the long run, about half of the actual values would be lower than their median and half would be higher.

Uncertainty distributions used in reliability analysis tend to be skewed; in such distributions, the instances of the actual value being above the median tend to increase the mean by more than the amount it is reduced by occasions when the actual value is below the median. Consequently, the mean of a such a parameter tends to be larger than the median.

The uncertainty distribution for the sum of two parameters is a convolution integral involving the uncertainty distributions for the separate parameters, provided that their uncertainties are not correlated. There is no simple procedure for estimating the parameters of the resulting distribution without considering the integral. Furthermore, if there is correlation between the parameters, it is necessary to use stochastic methods to determine the resulting distribution.

In this study, uncertainty distributions for switchover-related failures were propagated through event trees and fault trees with the Integrated Reliability and Risk Analysis System (IRRAS) computer program (Russell and McKay), using a stochastic process called Latin Hypercube Sampling, supplemented by manual methods where necessary. Uncertainty distributions for differences between two CDFs were calculated from their convolution. Other uncertainties in the cost/benefit analyses were treated with the revised FORECAST regulatory effects analysis software (Lopez and Sciacca), which uses convolution integral techniques.

All uncertainty distributions used in the current analysis and entered into the computer programs were either uniform or log-normal distributions. A uniform distribution has equally likely values between a minimum and maximum and zero probability outside of the defined range. A log normal distribution is such that the logarithm of the parameter has a normal distribution. Uncertainty distributions calculated by the computer programs could have any form; if it was necessary to perform a manual step using a computer-generated distribution, it was approximated by a log normal or uniform distribution. Such approximations always preserved the mean and any essential property, such as the sign of the 5th or 95th percentile. Within these constraints, the other percentiles were matched as closely as possible.

3.0 Method for Calculating Risk

3.1 Technical Approach

The present study was directed toward obtaining improved risk estimates for manual and automatic control systems for ECCS switchover to recirculation. Risk estimates were obtained by PRA methods, that is, by quantifying models that represent the failure logic of plant systems.

The licensee for the representative ECCS switchover systems has two 4-loop Westinghouse PWRs at the same site, with similar control rooms. Both plants were built with manual switchover, but one has been modified to a semiautomatic system. The licensee arranged for the authors to observe the manual switchover procedure at their simulator and provided current versions of the tagging procedures and both sets of EOPs.

The approach used in this study included the development of detailed human reliability models for both the manual and semiautomatic switchover procedures. The remainder of the plant failure logic model was taken from an existing PRA for a different plant. Each analysis, one for manual and one for semiautomatic ECCS switchover, uses a model that is a hybrid of two plants. Only switchover control failures were modified; valve reliabilities retained the values assigned in the existing PRA.

3.2 Selection of Plant PRA for Evaluation of Risk

The NRC has developed computer programs as aids in performing PRAs. These programs include the IRRAS software (Russell and McKay). This program includes functions that allow the user to quantify cut sets and to perform uncertainty analysis on the results.

This study used the Sequoyah Unit 1 PRA (Bertucio and Brown) for the plant failure logic model. The Sequoyah PRA is available in an electronic form compatible with the IRRAS risk analysis software, permitting modification and reevaluation without the need to manually enter data for a complete plant. Furthermore, the electronic data base includes the internal events cut sets and the event data, permitting reevaluation of the internal events CDF without repeating the Boolean manipulations of the entire fault tree model.

The next section of this report discusses the interface between the Sequoyah 1 PRA and the representative plant switchover control failure logic. The similarity of these PWRs simplifies the task of interfacing the models. These 4-loop Westinghouse PWRs were licensed within a year of each other. The ECCS systems have the same two-train design, with RHR pumps providing low-pressure injection and recirculation; both charging pumps and safety injection pumps provide high-pressure recirculation and take suction from the RHR pumps.

The Sequoyah PRA provides a comprehensive treatment of LOCAs. The four sizes of LOCA are large, medium, small, and very small. The last category includes reactor coolant pump seal LOCAs.

Finally, the Sequoyah PRA is supplemented by a back-end analysis (Gregory and Murfin). Core damage states represent outcomes of accident sequences. The internal events CDF is apportioned to the core damage states, and the expected public exposure is calculated for each state. Therefore, this study's comparison of risk may be converted from CDF to public exposure in person-rem.

3.3 Shutdown Risk

One disadvantage of the Sequoyah 1 PRA (and of most PRAs performed to date) is that it considers only accidents initiated during power operations. One of the vulnerabilities of an automatic system, especially in a plant that uses RHR pumps for low-pressure injection, is spurious switchover to take suction from a dry containment sump while the RHR system is performing its shutdown cooling function. This event could lead to pump damage and loss of core cooling; the analysis of this situation is beyond the scope of the present study. Appendix C includes some information relevant to that question. For this study, it is sufficient to note that automation can be planned such that this vulnerability is avoided and that the representative semiautomatic system does not have this vulnerability.

3.4 Method of Interfacing ECCS Switchover Failures with NUREG-1150

To make use of the NUREG-1150 cut sets for Sequoyah (Bertucio and Brown), the ECCS switchover model must produce a new set of distributions for existing basic events. Therefore, the first step was identification of those basic events in the NUREG-1150 Sequoyah PRA that represent or can be redefined to represent failures of ECCS switchover control. Although the containment spray system also requires manual action when the RWST reaches a low level, automation of that action was not considered in the present study. Figures 3.1, 3.2, and 3.3 show, respectively, the Safety Injection System, the Charging System, and the Low Pressure/Recirculation System for Sequoyah (Bertucio and Brown).

The failure model for a particular switchover control system consists of a collection of fault trees, called subtrees. The top event for each subtree is a redefined Sequoyah basic event. The subtree represents further refinement of the model in terms of basic switchover control failures.

Each of the subtrees was evaluated separately, and the calculated distributions were entered in IRRAS to replace the original Sequoyah data for basic events. The IRRAS software can then recalculate the mean CDF and its uncertainty.

For this procedure to be valid, the subtrees must be independent of each other. Therefore each basic switchover control failure must appear in only one of the subtrees.

3.5 ECCS Switchover Control Failures in NUREG-1150 PRA

The fault trees that were developed for the NUREG-1150 Sequoyah PRA contain twenty-one basic events that affect ECCS switchover control. However, the NUREG-1150 Sequoyah HRA concluded that certain manual failures are coupled such that one failure is completely dependent on the occurrence of another failure. Therefore, prior to the cut set analysis, eleven of the individual failures were replaced by seven coupled failures. In addition, credit was taken for a recovery action, which introduced the additional failure event for that recovery action. The result is that there are eighteen different basic events that are failures of switchover control and may appear in a NUREG-1150 Sequoyah cut set. These eighteen NUREG-1150 basic events are listed in Table 3.1.

An interlock fault for flow control valves 63-175, 63-3, or 63-4 has the same effect in the Sequoyah model as failure to operate the valve. However, an interlock fault for valve 63-72 or 63-73 is not equivalent to failure to operate that valve; rather, it has the effect of failing to operate valve 74-3 or 74-21, respectively.

In the NUREG-1150 model of the Sequoyah ECCS, coupled failure to activate all Safety Injection (SI) miniflow valves inhibits opening of the valves from LPSI to HPSI and therefore fails high-pressure recirculation. For the NUREG-1150 Sequoyah PRA, the definition of this human error was expanded to include failure to diagnose the need to begin switchover at the appropriate time. The probability of diagnosis error was based on the time available, leading to three separate values, each with its own nomenclature in Table 3.1. S_2 identifies a small LOCA. S_3 and S_3O_c are a very small LOCA, with and without operator control of containment sprays.

In the present study, the three basic events representing coupled operator failure to close miniflow valves were no longer defined to include diagnosis errors; they therefore all have the same probability.

For the representative plant, diagnosis errors were assumed to fail switchover of both LPSI trains. To reflect the varying time available, new basic events were defined and added to the IRRAS data base for Sequoyah.

The detailed models of switchover control at the representative plant contain some failure modes of switchover control that are not in Table 3.1. Some of these other failure modes have the same effects as events that do appear in Table 3.1; these failure modes can be included by expanding the definitions of the events. However, the following control failures have effects for which there is no equivalent in Table 3.1:

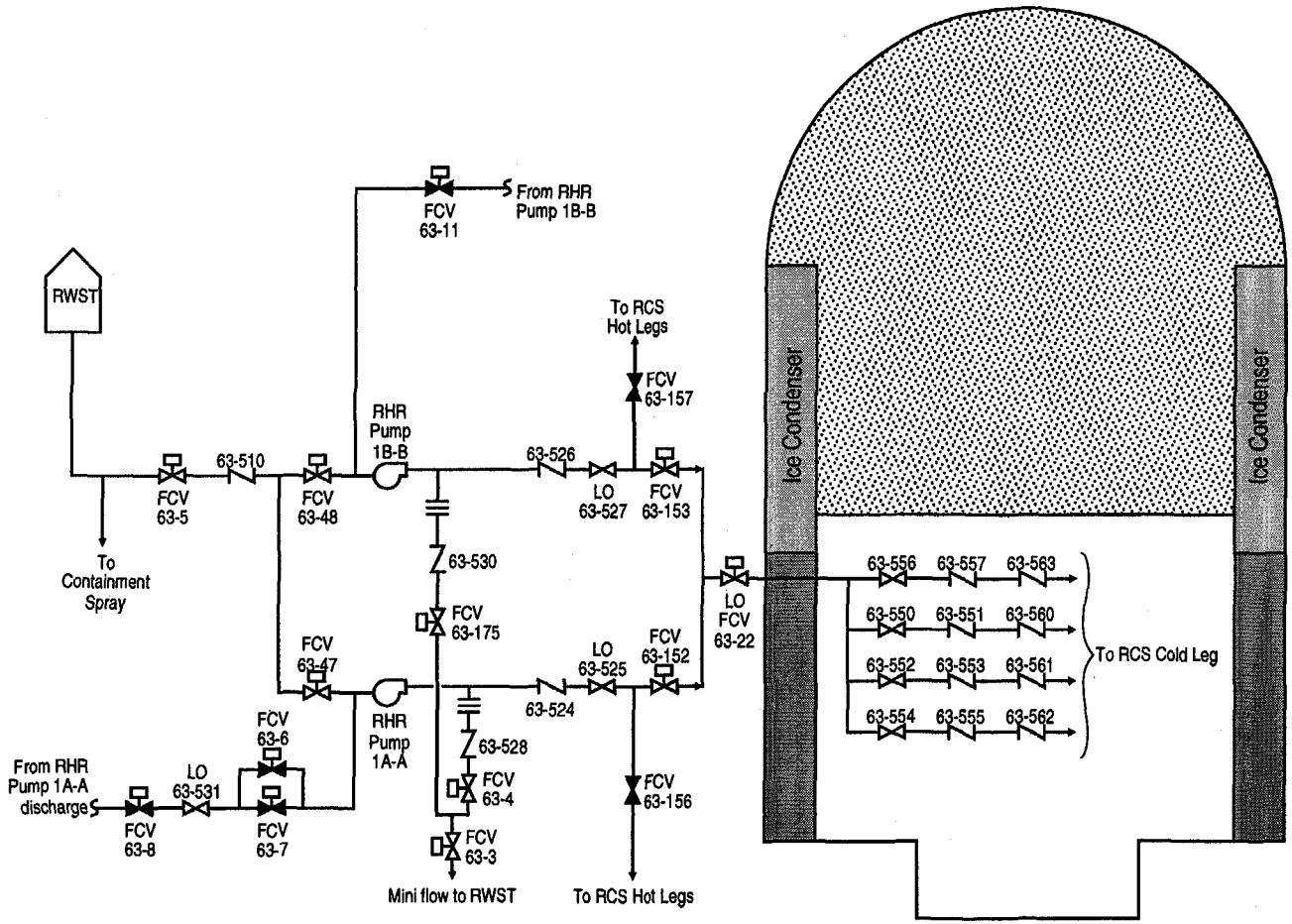

Figure 3.1 Simplified Schematic of Safety Injection System

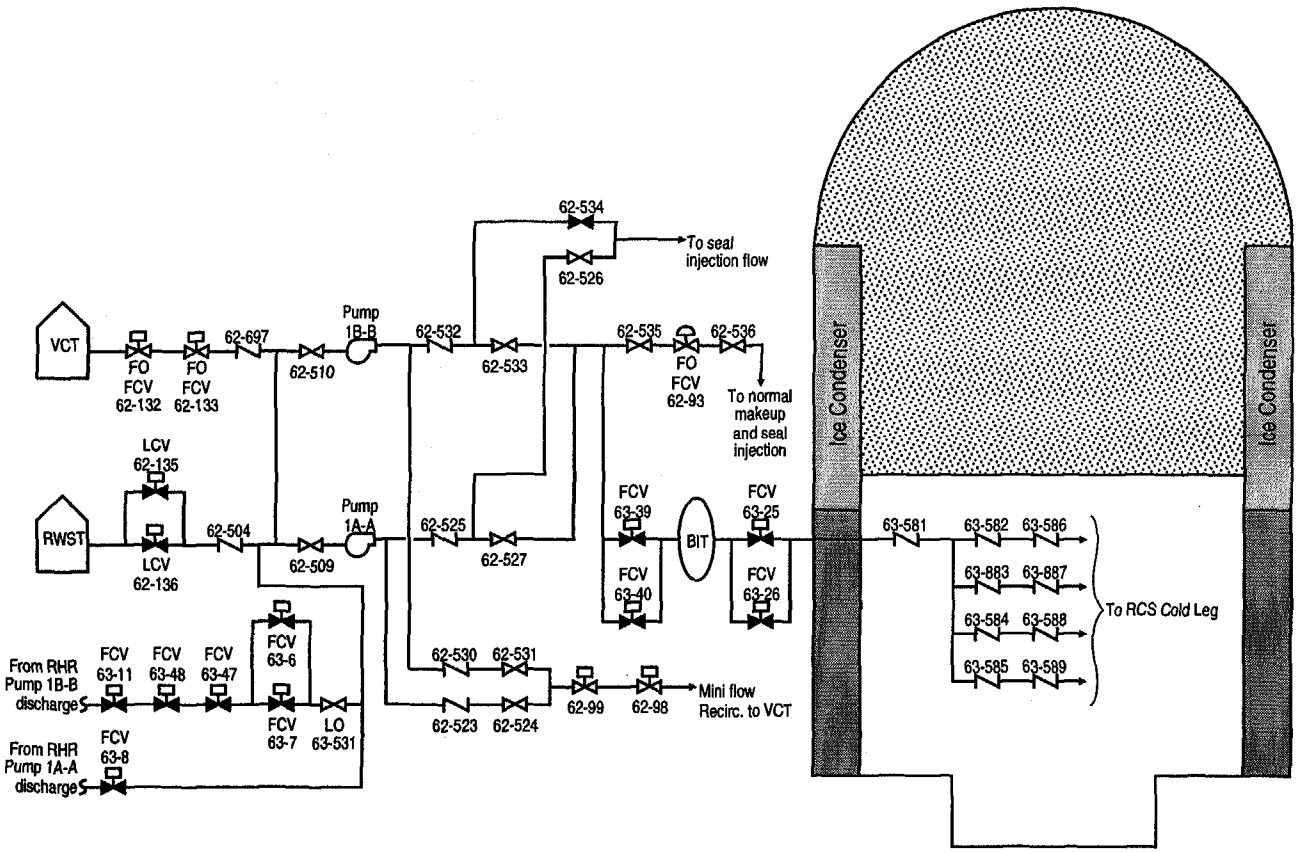

Figure 3.2 Simplified Schematic of Charging System

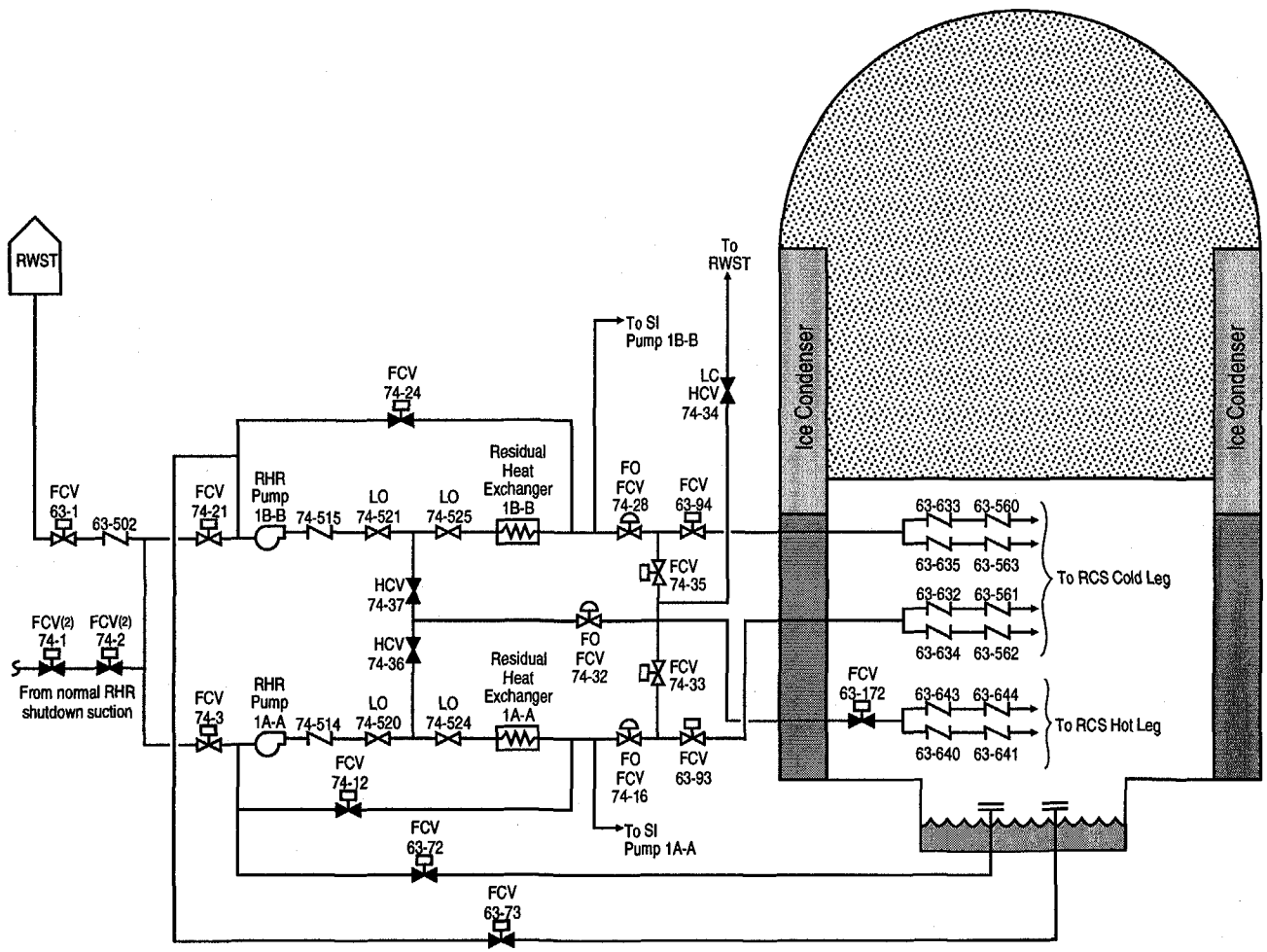

Figure 3.3 Simplified Schematic of the Low Pressure Injection/Recirculation System

Table 3.1 NUREG-1150 Sequoyah Basic Events Involving Switchover Control Failures

Nomenclature	NUREG-1150 Sequoyah PRA Description
HPR-XHE-FO-631	Operator Fails to Close FCV 63-1
HPR-XHE-FO-635	Operator Fails to Close HPR FCV 63-5
HPR-XHE-FO-CHISL	Operator Fails to Close CHG System Suction Valves from RWST
HPR-XHE-FO-SIMIN	Operator Fails to Close SI Miniflo to RWST (S_1 or S_2)
HPR-XHE-FO-SIMN1	Operator Fails to Close SI Miniflo to RWST (S_3)
HPR-XHE-FO-SIMN2	Operator Fails to Close SI Miniflo to RWST (S_3O_c)
HPR-XHE-FO-V6V7	Operator Fails to Open HPR FCVS 63-6, -7
HPR-XHE-FO-V8V11	Operator Fails to Open HPR FCVS 63-8, -11
LPR-ACT-FA-TRNA	FCV 63-72 Does Not Receive Open Signal
LPR-ACT-FA-TRNB	FCV 63-73 Does Not Receive Open Signal
LPR-ICC-NO-63175	LPR FCV 63-175 Interlock Faults
LPR-ICC-NO-633	LPR FCV 63-3 Interlock Faults
LPR-ICC-NO-634	LPR FCV 63-4 Interlock Faults
LPR-ICC-NO-6372	LPR FCV 63-72 Interlock Faults
LPR-ICC-NO-6373	LPR-FCV 63-73 Interlock faults
LPR-XHE-FO-CHR	Operator fails to establish CCW TO HX
RA7	FL TO MAN effect ECCS Sump Recirculation Switchover
RWT-XHE-MSCAL	Miscalibration of RWST level sensors

- Independent operator failure to close suction valve from RWST to one LPSI train (manual only).
- Independent operator failure to close one CHG suction valve from RWST.
- Independent operator failure to open one valve for HPSI suction from LPSI discharge (63-8 or 63-11).
- Independent operator failure to open one valve for HPSI suction from opposite train (63-6 or 63-7) (manual only).

In order to treat these failures to operate valves, eight basic events for valve failures were redefined to include operator failure to open or close the valve. These are listed in Table 3.2.

Therefore, there are 29 basic events in the modified Sequoyah cut sets that provide an interface for the switchover control failure logic. These 29 events are

Table 3.2 NUREG-1150 Sequoyah Valve Failures Redefined to Include Operator Errors

Nomenclature	NUREG-1150 Sequoyah PRA Description
HPR-MOV-CC-6311	HPR FCV 63-11 Fails to Open
HPR-MOV-CC-636	HPR FCV 63-6 Fails to Open
HPR-MOV-CC-637	HPR FCV 63-7 Fails to Open
HPR-MOV-CC-638	HPR FCV 63-8 Fails to Open
HPR-MOV-OO-62135	HPR LCV 62-135 Fails to Close
HPR-MOV-OO-62136	HPR LCV 62-136 Fails to Close
LPI-MOV-OO-7421	LPI FCV 74-21 Fails to Close
LPI-MOV-OO-743	LPI FCV 74-3 Fails to Close

listed in Tables 3.3 through 3.5, with the NUREG-1150 nomenclature for each event and the definition of the event for this study. In Table 3.3 the definitions are stated in terms of control signals, to avoid separate definitions for the manual and semiautomatic controls.

There is a one-to-one correspondence between the Sequoyah 1 and representative plant valves, except for the SI miniflow valves. The representative plant has only two such valves, one less than Sequoyah, and they are configured differently, as shown in Figure 4.1. To complete the interface, this analysis redefined the control room and EOP to include operation of an additional valve, 2SJ67X, as follows:

Sequoyah	Rep. Plant	Lockout?
63-3	2SJ67	Yes
63-4	2SJ68	Yes
63-175	2SJ67X	Yes

Table 3.3 Events from Extended NUREG-1150 Sequoyah Model Used in Both Failure Models

Nomenclature	Definition for This Study (Representative Plant Valve Identifiers)
HPR-MOV-CC-6311	Valve 21SJ45 does not open [valve or control failure]
HPR-MOV-CC-638	Valve 22SJ45 does not open [valve or control failure]
HPR-MOV-OO-62135	Valve 2SJ1 does not close [valve or control failure]
HPR-MOV-OO-62136	Valve 2SJ2 does not close [valve or control failure]
HPR-XHE-FO-631	Valve 2SJ69 does not receive close signal
HPR-XHE-FO-635	Valve 2SJ30 does not receive close signal
HPR-XHE-FO-CHISL	Common cause failure of close signals to valves 2SJ1 and 2SJ2
HPR-XHE-FO-SIMIN	Common cause failure of close signals to valves 2SJ67, 2SJ68, and 2SJ67X (S_1 or S_2)
HPR-XHE-FO-SIMN1	Common cause failure of close signals to values 2SJ67, 2SJ68, and 2SJ67X (S_3)
HPR-XHE-FO-SIMN2	Common cause failure of close signals to valves 2SJ67, 2SJ68, and 2SJ67X (S_3O_C)
HPR-XHE-FO-V8V11	Common cause failure of open signals to valves 21SJ45 and 22SJ45
L3-RWSTL-OP	Operator fails to diagnose the need to switchover at the appropriate time (S_1 or S_2)
L3-RWSTL-OP1	Operator fails to diagnose the need to switchover at the appropriate time following a large LOCA
L3-RWSTL-OP2	Operator fails to diagnose the need to switchover at the appropriate time (S_3O_C)
LPR-ACT-FA-TRNA	Single-point failure of LPSI switchover control for train A [includes initiation failure, failures of signals to 21CC16 and 21SJ44, and both control and pump failures to stop and restart 21RHR pump if required]
LPR-ACT-FA-TRNB	Single-point failure of LPSI switchover control for train B
LPR-ICC-NO-63175	Valve 2SJ67X does not receive close signal
LPR-ICC-NO-633	Valve 2SJ67 does not receive close signal
LPR-ICC-NO-634	Valve 2SJ68 does not receive close signal
RWT-XHE-MSCAL	Common cause failure of LPSI switchover for trains A and B [includes miscalibration of RWST level sensors, diagnosis and initiation failures, common cause failures to signal SJ44 valves, and common cause control and pump failures to stop and restart RHR pumps if required]

Table 3.4 NUREG-1150 Sequoyah Basic Events Used Only in the Manual Switchover Model

Nomenclature	Definition for This Study (Representative Plant Valve Identifiers)
HPR-MOV-CC-636	Valve 21SJ113 does not open [valve failure or operator error]
HPR-MOV-CC-637	Valve 22SJ113 does not open [valve failure or operator error]
HPR-XHE-FO-V6V7	Common cause failure of open signals to valves 21SJ113 and 22SJ113
LPI-MOV-OO-7421	Valve 22RH4 does not close [valve failure or operator error]
LPI-MOV-OO-743	Valve 21RH4 does not close [valve failure or operator error]
LPR-XHE-FO-CHR	Common cause failure of open signals to valves 21CC16 and 22CC16

Table 3.5 NUREG-1150 Sequoyah Basic Events Used Only in the Semiautomatic Switchover Model

Nomenclature	Definition for This Study (Representative Plant Valve Identifiers
LPR-ICC-NO-6372	Valve 21SJ44 interlock faults
LPR-ICC-NO-6373	Valve 22SJ44 interlock faults
RA7	Failure to manually accomplish LPSI switchover for a train after automatic switchover fails for that train

4.0 Design of a Representative Semiautomatic Switchover System

4.1 System Overview

This section describes one possible system design for automating ECCS switchover to recirculation, based on a design for Salem Unit 2. After a brief system overview, the specific required modifications are discussed.

Each of the two Salem PWR units uses two RHR trains to perform the LPSI function. The normal charging pumps and the safety injection pumps accomplish HPSI. Unit 1 was licensed in 1976 with manual switchover. The licensee submitted a conceptual design for its semiautomatic system for Unit 2 in 1980 (Mittl). The submittal included design criteria, an evaluation of switchover automation, the conceptual design of the proposed semiautomatic system, a failure mode and effects analysis (FMEA) of the proposed system, and a summary evaluation of the design. The switchover steps identified included the following:

- Open sump to suction from LPSI pumps;
- Isolate LPSI pumps from RWST;
- Open component cooling water to LPSI heat exchangers;
- Open HPSI pump suction cross-over header;
- Close LPSI discharge cross-connect valves;
- Isolate HPSI miniflow;
- Open LPSI pump discharge lines to suction from HPSI pumps.

Each step represents a pair of operations, one on each train. These steps were evaluated to identify advantages and disadvantages of automation. The results of the licensee's evaluation are summarized in Table 4.1. The licensee proposed to automate the first four steps, including the addition of check valves to remove the potential for an unacceptable single failure from automating the first step. The licensee stated that automating beyond this extent would make the switchover design susceptible to unacceptable single failures that may reduce ECCS flow to the RCS below minimum requirements.

The evaluation also determined that the steps that cannot be automated are few in number and can be implemented based only on operator verification that switchover to recirculation is required; that is, RWST level is low and the sump level is adequate to support RHR pump net positive suction head (NPSH) requirements. The switchover procedure can be structured to minimize and emphasize the operator actions that must be performed to protect all ECCS pumps from loss of suction source.

The contents of Table 4.1 were generated by the licensee. This information demonstrates the types of consideration that a licensee must evaluate, and does not necessarily reflect judgment related to the present study.

4.2 Modifications for Switchover

Figure 4.1 is a schematic of the ECCS at Salem Unit 2 showing the check valves that were used for the postulated design of the semiautomatic system. To eliminate unacceptable single failures associated with opening the sump valves, the initial design included check valves in each of the RHR pump suction lines from the RWST and the containment sump. Additional check valves were included for the RWST suction lines to deal with the more subtle effects of the failure of one sump valve to open on demand. Continuous operation of the RHR pumps requires that the sump valves be opened before the RWST is isolated. Because both of the RWST suction lines are connected to a common supply from the RWST, an RHR pump without access to its sump may take suction from the other sump by reverse flow through the other RWST line. Under such conditions, both pumps could be damaged, and all ECCS function would be lost. Addition of the check valves minimizes the likelihood of this type of occurrence.

The possibility of spurious automatic transfer to an empty recirculation sump was reduced by designing the system as a two-train system which meets the single failure criterion. In addition, actuation signals from four RWST level transmitters were combined into a two-out-of-four logic for each train, thus reducing the possibility of an inadvertent transfer due to a failed instrument. Furthermore, the actuating devices were designed with energize-to-

Table 4.1 Example Licensee Considerations in Implementing Automatic Switchover (Mittl)

Step	Advantages of Automation	Disadvantages of Automation
Open sump to suction from LPSI pumps.	Provides sump suction/NPSH for RHR pumps without operator action.	Unacceptable single failure: Failure of one sump valve to open on demand could permit both RHR pumps to draw suction from one sump line and damage both pumps. Spurious (early) opening could damage one RHR pump. Opening could permit potential backflow from RWST to sump, requiring a larger transfer allowance and therefore affecting RWST sizing
Isolate LPSI pumps from RWST.	Minimizes RWST outflow following sump valve opening without operator action.	Spurious (early) sequential automatic closure before adequate water exists in sump could damage one RHR pump.
Open component cooling water to LPSI heat exchangers.	Provides component cooling water to RHR HX without operator action. No operator decision/verification required.	none
Open HPSI pump suction crossover header.	Opens SI/CHG pump suction crossover header without operator action. No operator decision/verification required.	none
Close LPSI discharge crossconnect valves.	Closes RHR discharge crossconnect valves without operator action.	Unacceptable single failure: Spurious (early) sequential automatic closure results in damage to one RHR pump and reduces ECCS flow below minimum safeguards.
Isolate HPSI miniflow.	Isolates SI miniflow without operator action.	Unacceptable single failure: Spurious (early) sequential automatic closure could damage both SI pumps, reducing ECCS flow below minimum safeguards.
Open LPSI pump discharge lines to suction from HPSI pumps.	Provides suction/NPSH for SI and CHG pumps from RHR pump without operator action.	Closure of RHR discharge crossconnect valves and isolation of SI miniflow are required to be completed before opening LPSI discharge to suction from HPSI.

actuate logic to prevent premature actuation due to a failed or malfunctioning transmitter.

Finally, an interlock prevents automatic actuation of switchover under any plant operating condition which does not normally result in safety injection. For cost estimating purposes, the design modifications for a semiautomatic ECCS switchover system are summarized in Table 4.2.

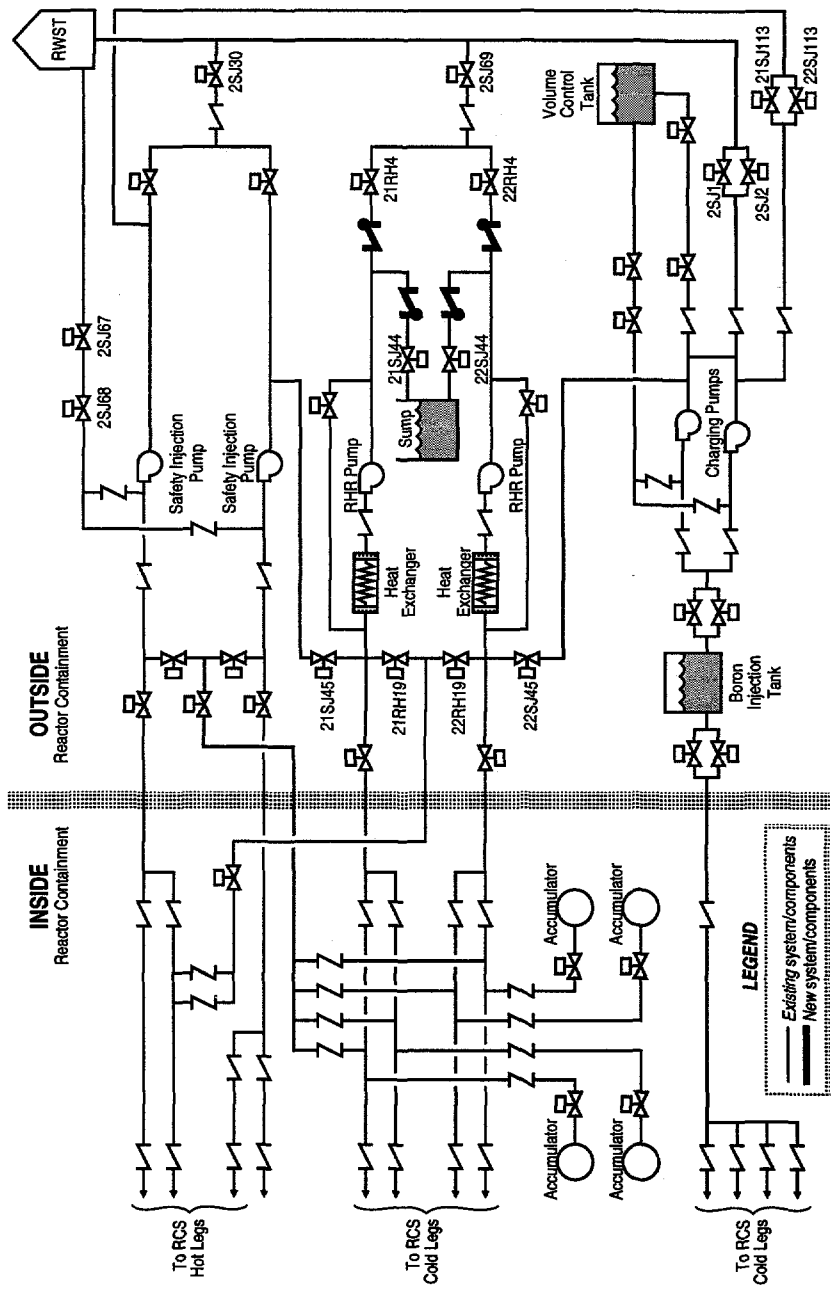

Figure 4.1 Salem Unit 2 ECCS Proposed Design for Semiautomatic Switchover

Table 4.2 Summary of Design Modifications (Manual to Semiautomatic Switchover)

Modification	Description
Add Sump Check Valves (Verify adequate NPSH)	Install check valve between the pump suction connection and the containment sump isolation valve in each line. Precludes draining of the RWST into the sump if isolation valves open inadvertently.
Add RWST Check Valves (Verify adequate NPSH)	Install check valve in pump suction and before connection point of sump suction piping. Precludes both RHR pumps attempting to take suction from one sump line if one sump isolation valve fails to open.
Automate Switchover Logic	Four RWST level transmitters provide input signals to solid-state Protection System. 2 out of 4 Low-Level Logic Bistables normally de-energized. Switchgear sequence signal reset capability in control room. Manual actuation at the system level not provided.
Upgrade Sump Isolation Valves	Provide lockout of power to prevent spurious opening. Provide interlock to prevent opening unless RWST to RHR pump suction valve is closed.
Develop New Operating Procedures	Incorporate new procedures and provide operator training.

5.0 Failure Models for ECCS Switchover Control

This section defines failure models for manual and semiautomatic ECCS switchover. The descriptions are in the form of subtrees that define *NUREG-1150* Sequoyah basic events in terms of Representative Plant switchover control failures.

5.1 Failure Model for Manual Switchover Control

There are 26 NUREG-1150 events in Tables 3.3 and 3.4 that apply to manual systems and might have required subtrees. However, the 15 basic events in Table 5.1 were not refined further. Another eight of the NUREG-1150 basic events were each expanded into an OR gate with two Representative Plant basic events. The algebraic representations for these eight subtrees appear in Table 5.2.

The remaining three NUREG-1150 basic events were developed as subtrees in Figures 5.1 through 5.3 as follows:

Fig. 5.1 RWT-XHE-MSCAL

Fig. 5.2 *LPR-ACT-TRNA*

Fig. 5.3 LPR-ACT-TRNB

In these three subtrees, failure of a pump to stop on demand was omitted because the failure probability for stopping was judged to be small relative to the probability that the pump fails to restart.

This model does not include coupled failures to operate valves 21RH4 and 22RH4, because the NUREG-1150 model did not contain any basic event that has an effect equivalent to this common cause failure. To account for the possibility of the common cause failure, the probabilities of the individual failures were adjusted such that their product accounted for the corresponding common cause event. The impact of this approximation on the results of this study was small because these valves are redundant to valve 2SJ69; common failure of 21RH4 and 22RH4 is not a single-point failure of LPSI switchover.

Table 5.1 Basic Events that Were Not Refined Further for Manual Model

HPR-XHE-FO-631	L3-RWSTL-OP
HPR-XHE-FO-635	L3-RWSTL-OP1
HPR-XHE-FO-CHISL	L3-RWSTL-OP2
HPR-XHE-FO-SIMIN	LPR-XHE-FO-CHR
HPR-XHE-FO-SIMN1	LPR-ICC-NO-63175
HPR-XHE-FO-SIMN2	LPR-ICC-NO-633
HPR-XHE-FO-V6V7	LPR-ICC-NO-634
HPR-XHE-FO-V8V11	

Table 5.2 Algebraic Representations of Eight Subtrees for Manual Switchover Model

HPR-MOV-CC-6311	=HP-21SJ45O-OP (Op fails to open 21SJ45) or HP-21SJ45O-HW (Valve fails to open)
HPR-MOV-CC-636	=HP-21SJ113O-OP (Op fails to open 21SJ113) or HP-21SJ113O-HW (Valve fails to open)
HPR-MOV-CC-637	=HP-22SJ113O-OP(Op fails to open 22SJ113) or HP-22SJ113O-HW (Valve fails to open)
HPR-MOV-CC-638	=HP-22SJ45O-OP (Op fails to open 22SJ45) or HP-22SJ45O-HW (Valve fails to open)
HPR-MOV-OO-62135	=HP-2SJ1C-OP (Op fails to close 2SJ1) or HP-2SJ1C-HW (Valve fails to close)
HPR-MOV-OO-62136	=HP-2SJ2C-OP (Op fails to close 2SJ2) or HP-2SJ2C-HW (Valve fails to close)
LPI-MOV-OO-7421	=LP-22RH4C-OP (Op fails to close 22RH4) or LP-22RH4C-HW (Valve fails to close)
LPI-MOV-OO-743	=LP-21RH4C-OP (Op fails to close 21RH4) or LP-21RH4C-HW (Valve fails to close)

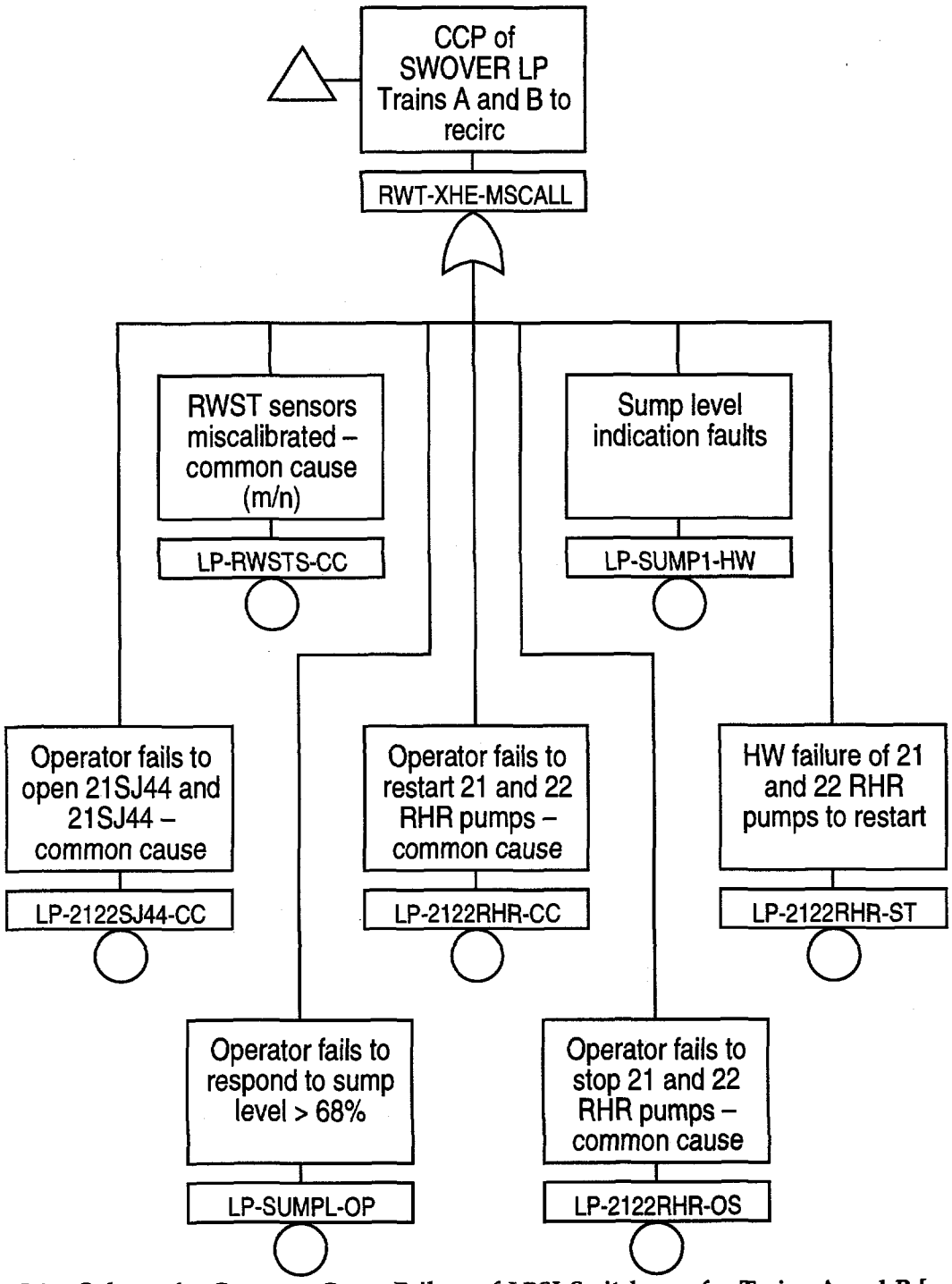

Figure 5.1 Subtree for Common Cause Failure of LPSI Switchover for Trains A and B [manual]

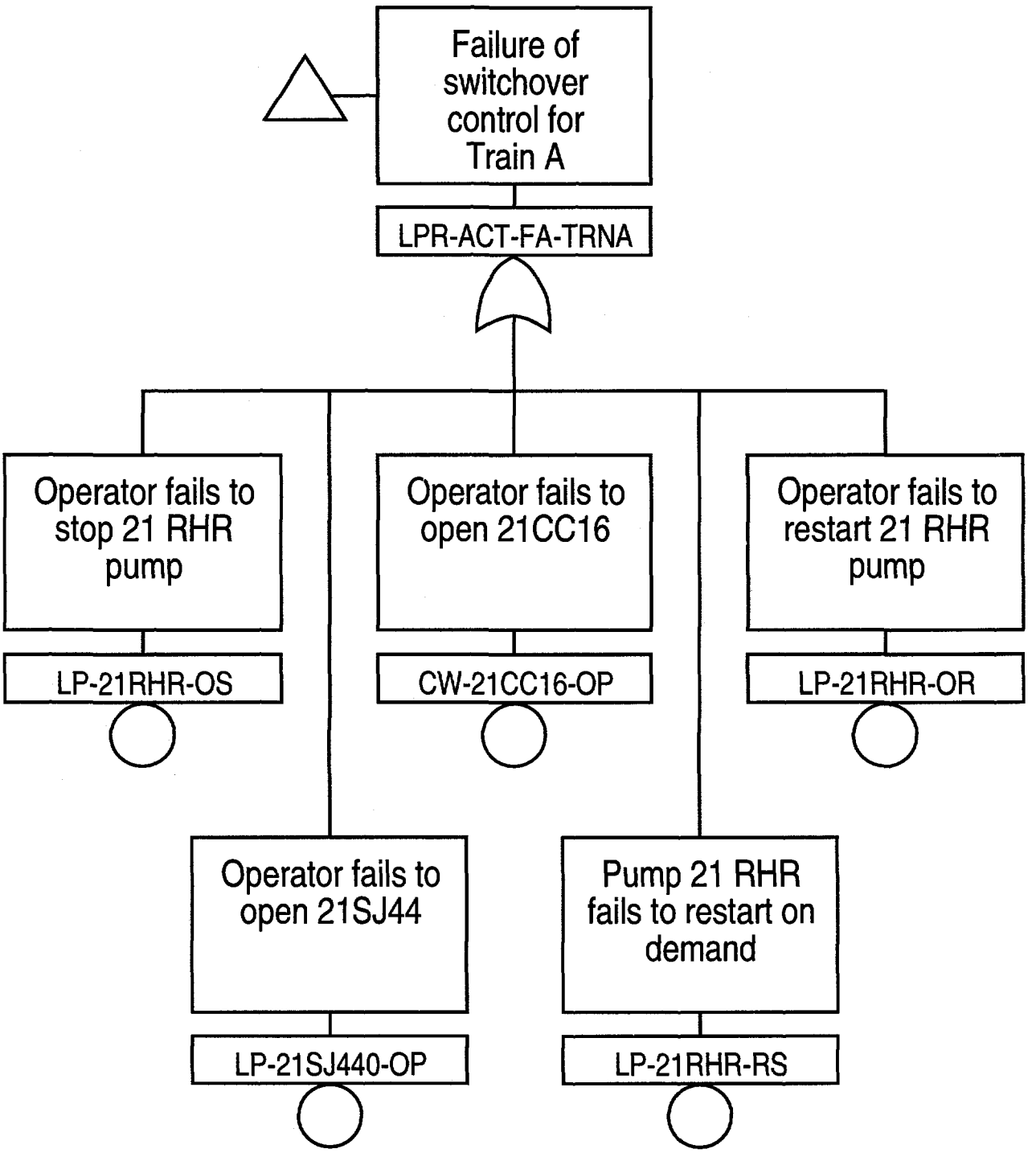

Figure 5.2 Subtree for Single-Point Failure of LPSI Switchover for Train A [manual]

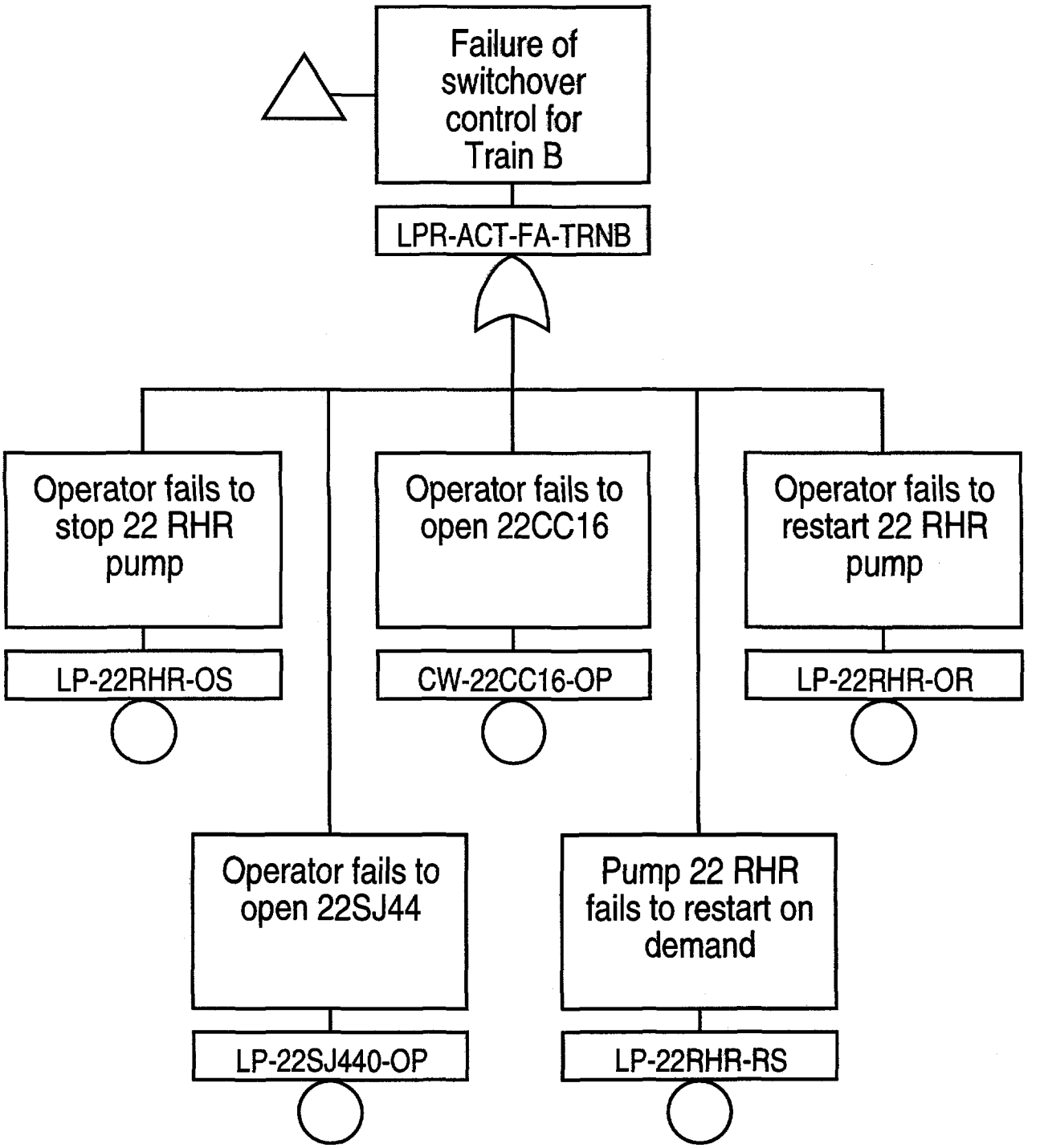

Figure 5.3 Subtree for Single-Point Failure of LPSI Switchover for Train B [manual]

The failure model for manual switchover contains 48 Representative Plant basic events. For the twelve valve and pump failures and the one maintenance error, probability distributions were based on NUREG-1150 event failure data, as shown in Table 5.3. The abbreviation "EF" denotes the error factor that corresponds to each event's mean value. Sump level indication faults were not part of the NUREG-1150 model; the failure probability for such an event was assumed to be the same as that for another instrumentation fault, undetected low RWST level at accident initiation. The task of the reliability analysis for the manual system was to estimate probabilities for the operator errors listed in Table 5.4.

The remaining NUREG-1150 Sequoyah basic event, RWT-XHE-MSCAL, was developed as a subtree in Figure 5.4. The NUREG-1150 study omitted certain failures because their probabilities at Sequoyah are negligible compared to those of miscalibration of multiple RWST water level sensors and common cause failure of the sump valves. Consistent with that approach, the subtree in Figure 5.4 omits the following failures:

- miscalibration of multiple sump level sensors,
- concurrent unavailability of multiple analog level instrumentation channels, and
- independent failures of a sump valve and a protective check valve.

Table 5.3 NUREG-1150 Basic Events Appearing in Manual Switchover Subtrees

Subtree Nomenclature	Description (Sequoyah valve identifiers)	NUREG-1150 Data Base Entry	Probability Distribution	
			Mean	EF
HP-21SJ113O-HW	HPR FCV 63-6 Fails to open	HPR-MOV-CC-636	0.003	10
HP-21SJ45O-HW	HPR FCV 63-11 Fails to open	HPR-MOV-CC-6311	0.003	10
HP-22SJ113O-HW	HPR FCV 63-7 Fails to open	HPR-MOV-CC-637	0.003	10
HP-22SJ45O-HW	HPR FCV 63-8 Fails to open	HPR-MOV-CC-638	0.003	10
HP-2SJ1C-HW	HPR LCV 62-135 Fails to close	HPR-MOV-OO-62135	0.003	10
HP-2SJ2C-HW	HPR LCV 62-136 Fails to close	HPR-MOV-OO-62136	0.003	10
LP-2122RHR-ST	CC Failure of LPI MDPS	LPI-CCF-FS-1AABB	0.00045	---
LP-21RH4C-HW	LPI FCV 74-3 Fails to close	LPI-MOV-OO-743	0.003	10
LP-21RHR-RS	LPI MDP 1A-A Fails to start	LPI-MDP-FS-1AA	0.003	10
LP-22RH4C-HW	LPI FCV 74-21 Fails to close	LPI-MOV-OO-7421	0.003	10
LP-22RHR-RS	LPI MDP 1B-B Fails to start	LPI-MDP-FS-1BB	0.003	10
LP-RWSTS-CC	Miscalibration of RWST level sensors	RWT-XHE-MSCAL	0.0005	10
LP-SUMPI-HW	Sump level indication faults	ESF-ASL-FC-RWST1	0.00002	5

5.2 Failure Model for Semiautomatic Switchover

There are 23 NUREG-1150 events in Tables 3.3 and 3.5 that might have required subtrees for the semiautomatic system model. However, the 16 basic events listed in Table 5.5 were not refined further. Six NUREG-1150 events were each expanded into an OR gate with two Representative Plant basic events. The algebraic representations for these subtrees appear in Table 5.6

The failure model for semiautomatic manual switchover contained 31 Representative Plant basic events. For five hardware failures and the one maintenance error, probability distributions were based on the NUREG-1150 data base, as shown in Table 5.7. Sump level indication faults were not part of the NUREG-1150 model; the failure probability for such an event was assumed to be the same as that for another instrumentation fault, undetected low RWST level at accident initiation.

Table 5.4 Manual Switchover Control Failures Requiring Reliability Analysis

Event Nomenclature	Description (Representative Plant Valve Identifiers)
CW-21CC16-OP (22CC16)	Operator fails to open 21CC16 (22CC16)
HP-21SJ450-OP (22SJ45)	Operator fails to open 21SJ45 (22SJ45)
HP-21SJ113O-OP (22SJ113)	Operator fails to open 21SJ113 (22SJ113)
HP-2SJ1C-OP (2SJ2)	Operator fails to close 2SJ1 (2SJ2)
L3-RWSTL-OP	Operator fails to enter EOP LOCA-3 (S_1 or S_2)
L3-RWSTL-OP1	Operator fails to enter EOP LOCA-3 (A)
L3-RWSTL-OP2	Operator fails to enter EOP LOCA-3 (S_3O_C)
LP-SUMPL-OP	Operator fails to respond to sump level > 68%
LP-2122RHR-OS	Operator fails to stop 21 & 22 RHR pumps (CC)
LPR-HE-FO-CHR	Operator fails to open 21CC16 & 22C16 (CC)
LP-2122SJ44-CC	Operator fails to open 21SJ44 & 22SJ44 (CC)
LP-2122RHR-CC	Operator fails to restart 21 & 22 RHR pumps (CC)
LP-21RHR-OS (22RHR)	Operator fails to stop 21 (22) RHR pump
LP-21SJ44O-OP (22SJ44)	Operator fails to open 21SJ44 (22SJ44)
LP-21RHR-OR (22RHR)	Operator fails to restart 21RHR (22RHR) pump
HPR-XHE-FO-631	Operator fails to close 2SJ69
HPR-XHE-FO-635	Operator fails to close 2SJ30
LP-21RH4C-OP (22RH4)	Operator fails to close 21RH4 (22RH4)
LPR-ICC-NO-633	Operator fails to close 2SJ67
LPR-ICC-NO-634 (63175)	Operator fails to close 2SJ68 (2SJ67X)
HPR-XHE-FO-CHISL	Operator fails to close 2SJ1 and 2SJ2 (CC)
HPR-XHE-FO-SIMIN	Operator fails to close 2SJ67, 2SJ68, & 2SJ67X (CC)
HPR-XHE-FO-SIMN1	Operator fails to close 2SJ67, 2SJ68, & 2SJ67X (CC)
HPR-XHE-FO-SIMN2	Operator fails to close 2SJ67, 2SJ68, & 2SJ67X (CC)
HPR-XHE-FO-V6V7	Operator fails to open 21SJ113 and 22SJ113 (CC)
HPR-XHE-FO-V8V11	Operator fails to open 21SJ45 and 22SJ45 (CC)

Table 5.5 Basic Events that Were Not Refined Further for Semiautomatic Model

HPR-XHE-FO-631	L3-RWSTL-OP1
HPR-XHE-FO-635	L3-RWSTL-OP2
HPR-XHE-FO-CHISL	LPR-ICC-NO-63175
HPR-XHE-FO-SIMIN	LPR-ICC-NO-633
HPR-XHE-FO-SIMN1	LPR-ICC-NO-634
HPR-XHE-FO-SIMN2	LPR-ICC-NO-6372
HPR-XHE-FO-V8V11	LPR-ICC-NO-6373
L3-RWSTL-OP	RA7

Table 5.6 Algebraic Representations of Six Subtrees for Semiautomatic Switchover Model

LPR-ACT-FA-TRNA	= LP-21SJ44A-OP (Op fails to arm 21SJ44) or LP-LOGICA-HW (Logic board fails)
LPR-ACT-FA-TRNB	= LP-22SJ44A-OP (Op fails to arm 22SJ44) or LP-LOGICB-HW (Logic board fails)
HPR-MOV-CC-6311	= HP-21SJ45O-OP (Op fails to open 21SJ45) or HP-21SJ45O-HW (Valve fails to open)
HPR-MOV-CC-638	= HP-22SJ45O-OP (Op fails to open 22SJ45) or HP-22SJ45O-HW (Valve fails to open)
HPR-MOV-OO-62135	= HP-2SJ1C-OP (Op fails to close 2SJ1) or HP-2SJ1C-HW (Valve fails to close)
HPR-MOV-OO-62136	= HP-2SJ2C-OP (Op fails to close 2SJ2) or HP-2SJ2C-HW (Valve fails to close)

Six other basic events are hardware failures, namely:

LPR-ICC-NO-CC
LPR-ICC-NO-6372
LPR-ICC-NO-6373
LP-LOGIC-CC
LP-LOGICA-HW
LP-LOGICB-HW

These are failures of equipment that would be added to modify a manual system to make it semiautomatic. Because their probabilities are central to a comparison of the two alternatives, their NUREG-1150 values were reconsidered as part of the reliability analysis for the semiautomatic system.

The task of the human reliability analysis for the semiautomatic system was to estimate probabilities for the operator errors listed in Table 5.8.

Table 5.7 NUREG-1150 Basic Events Appearing in Semiautomatic Switchover Subtrees

Subtree Nomenclature	Description (Sequoyah valve identifiers)	NUREG-1150 Data Base Entry	Probability Distribution	
			Mean	EF
HP-21SJ45O-HW	HPR FCV 63-11 Fails to Open	HPR-MOV-CC-6311	0.003	10
HP-22SJ45O-HW	HPR FCV 63-8 Fails to Open	HPR-MOV-CC-638	0.003	10
HP-2SJ1C-HW	HPR LCV 62-135 Fails to Close	HPR-MOV-OO-62135	0.003	10
HP-2SJ2C-HW	HPR LCV 62-136 Fails to Close	HPR-MOV-OO-62136	0.003	10
LP-RWSTS-CC	Miscalibration of RWST Level Sensors	RWT-XHE-MSCAL	0.0005	10
LP-SUMPI-HW	Sump Level Indication Faults	ESF-ASL-FC-RWST1	0.00002	5

Table 5.8 Semiautomatic Switchover Manual Failures Requiring Reliability Analysis

Event Nomenclature	Description (Representative Plant Valve Identifiers)
HP-21SJ450-OP (22SJ45)	Operator fails to open 21SJ45 (22SJ45)
HP-2SJ1C-OP (2SJ2)	Operator fails to close 2SJ1 (2SJ2)
L3-RWSTL-OP	Operator fails to enter EOP LOCA-3 (S_1 or S_2)
L3-RWSTL-OP1	Operator fails to enter EOP LOCA-3 (A)
L3-RWSTL-OP2	Operator fails to enter EOP LOCA-3 (S_3O_C)
LP-SUMPL-OP	Operator fails to respond to sump level > 68%
LPR-XHE-FO-CHR	Operator fails to open 21CC16 & 22CC16 (CC)
LP-2122SJ44-CC	Operator fails to arm 21SJ44 & 22SJ44 (CC)
LP-21SJ44A-OP (22SJ44)	Operator fails to arm 21SJ44 (22SJ44)
HPR-XHE-FO-631	Operator fails to close 2SJ69
HPR-XHE-FO-635	Operator fails to close 2SJ30
LPR-ICC-NO-633	Operator fails to close 2SJ67
LPR-ICC-NO-634 (63175)	Operator fails to close 2SJ68 (2SJ67X)
HPR-XHE-FO-CHISL	Operator fails to close 2SJ1 and 2SJ2 (CC)
HPR-XHE-FO-SIMIN	Operator fails to close 2SJ67, 2SJ68, & 2SJ67X (CC)
HPR-XHE-FO-SIMN1	Operator fails to close 2SJ67, 2SJ68, & 2SJ67X (CC)
HPR-XHE-FO-SIMN2	Operator fails to close 2SJ67, 2SJ68, & 2SJ67X (CC)
HPR-XHE-FO-V8V11	Operator fails to open 21SJ45 and 22SJ45 (CC)

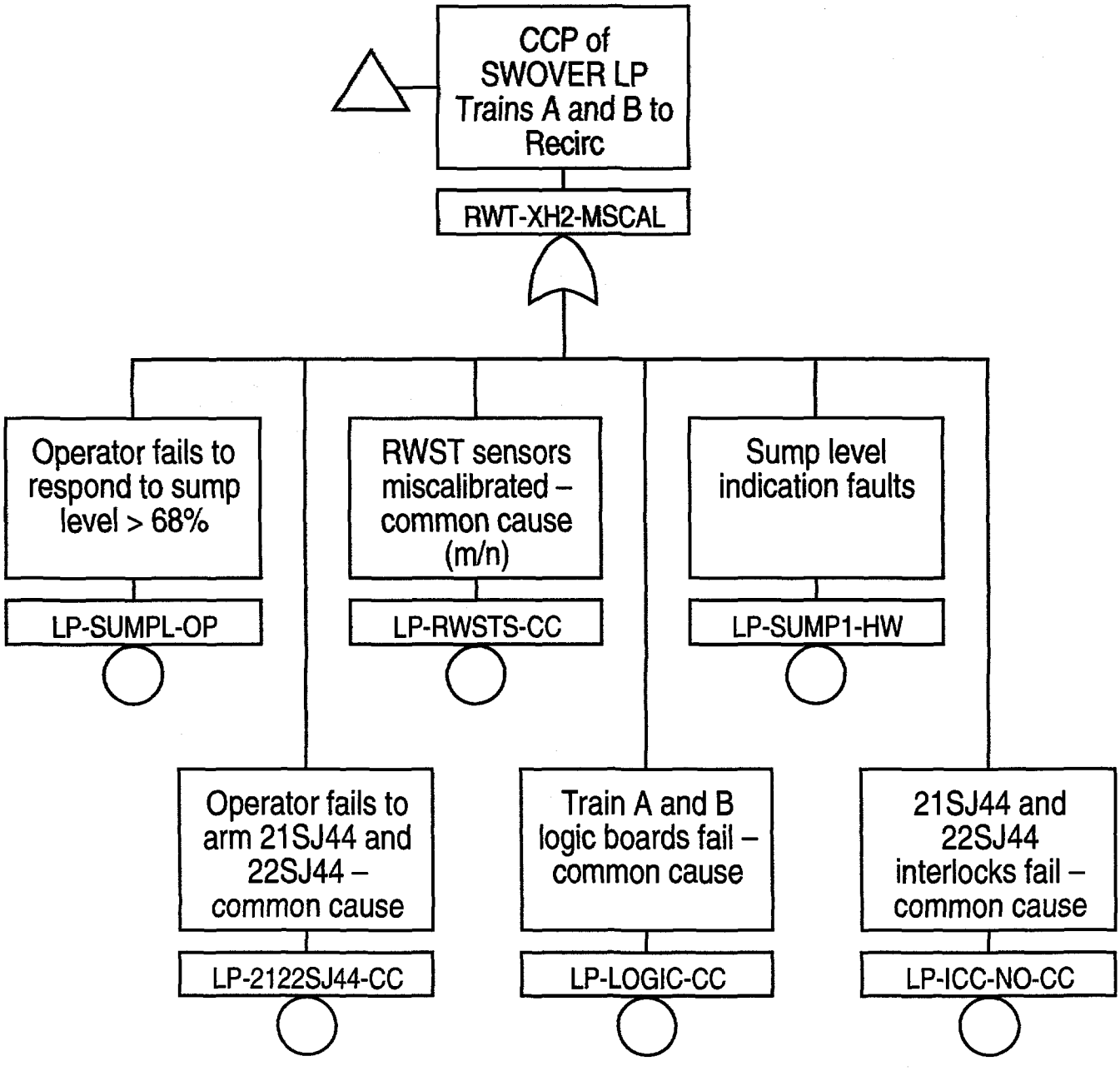

Figure 5.4 Subtree For Common Cause Failure of LPSI Switchover for Trains A and B [semiautomatic]

6.0 Reliability Analysis for ECCS Switchover

6.1 Reliability of Added Hardware

This subsection provides the basis for Table 6.1, which contains estimates for failure probabilities of hardware that would be added to convert a manual system to a semiautomatic system. This analysis does not include the added check valves because four batteries and therefore failure of the logic in both trains.

6.1.2 Sump Valve Interlock Faults

Failure of the interlock that closes the RWST valve when the sump valve is fully open is dominated by failure of the limit switch on the sump valve.

Table 6.1 Failure Probabilities for Added Hardware

Subtree Nomenclature	Probability Description	Distribution	
		Mean	EF
LP-LOGICA-HW	Train A logic board fails	0.00007	3
LP-LOGICB-HW	Train B logic board fails	0.00007	3
LP-LOGIC-CC	Train A & B logic boards fail - CC	0.00005	3
LPR-ICC-NO-6372	Valve 21SJ44 interlock faults	0.00004	5
LPR-ICC-NO-6373	Valve 22SJ44 interlock vaults	0.00004	5
LPR-ICC-NO-CC	21SJ44 & 22SJ44 interlocks fail - CC	Negligible	--

their failures were screened out in the previous section.

In the analysis of manually operated valves, faults were divided into instrumentation, human, and valve failures. Once the human has pressed the correct control, any failure to operate and to indicate successful operation is included in the valve failure probability. To retain consistency, failures of automatic controls included only failures to respond to correct information and transmit the correct signal. Failures of instrumentation channels and actuators were not considered to be failures of the automatic control.

6.1.1 Actuation Logic Faults

The failure rate for the logic circuit was calculated to be 1.1×10^{-8} per hour, as shown in Table 6.2, using standard formulas for a "Ground, Benign" environment (Department of Defense, MIL-HDBK-217F). However, this estimate is small compared to the common cause failure of the redundant batteries. A common cause methodology for batteries (NRC, NUREG-1150) yields a value of 5×10^{-5} per demand (error factor = 3) for common cause failure of all

However, that failure would also affect the indication of sump valve position and was therefore included in the sump valve failure probability.

The only interlock failure is the failure of the DC bus carrying the signal. This study used a failure probability of 4×10^{-5} per demand (error factor = 5), based on a failure rate of 1×10^{-7} per hour and a 30-day testing interval (NRC, NUREG-1150). Common cause failures to both interlocks were judged to be negligible in comparison with common cause failures of the logic in both trains.

6.2 Method for Human Reliability Analysis

This study considers each separate instruction of the EOP, the mechanism for each control, and the relationship of each control to its neighbors. This study includes a review and evaluation of available methods for Human Reliability Analysis (HRA), which is contained in Appendix D. Based on that evaluation, the method of the HRA Handbook (Swain and Guttmann) was selected for operation of controls and response to annunciators. The Sandia

Table 6.2 Reliability Analysis of Actuation Logic at 50°C

Component	Specifications	Failure Rate (per million hr)
4-gate array	MIL-M-38510, Class S, Hermetic CMOS flatpack	0.0015
4-gate array	same	0.0015
SPST relay	MIL-R-39016, Level R, Magnetic latching, Load current ratio <0.2, rated at 125°C	0.0007
9-pin connector	MIL-C-55302	0.0017
41 connections	Wrapped and soldered	0.0057
Total		**0.0111**

Recovery Model (Weston and Whitehead) was used for diagnosis.

The HRA Handbook provides a methodology to identify and quantify the potential for human error, with emphasis on tasks performed at nuclear power plants. It provides data, modeling, techniques, and a procedure, which together enable qualified analysts to perform HRAs.

The general method for the analysis of human performance consists of the following steps:

(1) Identify all the interactions of people with systems and components, i.e., the man-machine interfaces.

(2) Analyze these interfaces to see if the performance shaping factors (PSF) are adequate to support the tasks that people have to perform.

(3) Identify potential problem areas in equipment design, written procedures, plant policy and practice, people skills, and other factors likely to result in human error.

Any factor that influences human behavior is termed a PSF. PSFs can be external and internal. External PSFs include such items as architectural features, lighting, written procedures, accessibility of controls, readability of displays, etc. Internal PSFs include such items as training, experience, motivation, etc. External PSFs include a class known as stressors, which induce an internal PSF, stress. Stressors include such items as task load, distractions, threats (of catastrophe, loss of status, loss of job), etc. There are many other stressors, but these are the ones most relevant to this HRA.

This general method can be used as a qualitative or a quantitative analysis. The qualitative part is based on a descriptive and analytical technique known as task analysis. The quantitative part uses a human reliability technique to develop estimates of the effects of human performance on system criteria such as reliability and safety.

The HRA Handbook describes the Technique for Human Error Rate Prediction (THERP). The basic tool of THERP is an event tree. The limbs of the event tree show different human activities as well as different conditions or influences upon these activities. Conditional human error probabilities are assigned to each branch.

The HRA Handbook provides estimated human error probabilities and uncertainty bounds. It presents methods for assessing dependence among tasks or people. There is particular attention to manual operations in the control room of a nuclear power plant. The HRA Handbook lists nine PSFs that are related to controls, which are reproduced in Table 6.3.

6.3 Scope of HRA

The HRA addressed the probability of certain errors when carrying out a switchover from the Injection phase to the Recirculation phase of the ECCS at the Representative Plant. The assumption was made

Table 6.3 PSFs Related to Controls

(1)	Relationship of control to its display (includes physical distance and direction of movement)
(2)	Identification of control with its function (includes labeling, functional grouping of controls, and use of mimic panels)
(3)	Specific identification of control (includes control labeling - position, wording, and legibility of label; and control coding - color, shape, size, and position)
(4)	Anthropometrics (includes spacing, ease of reach, and ease of visual access)
(5)	Indicators on controls (includes types of indicators such as pointers and position marks, and visibility and distinctiveness of indicators)
(6)	Direction of motion (compliance with populational stereotypes)
(7)	Operator expectancies regarding layout of controls
(8)	Immediacy of feedback after control operation
(9)	Control room layout (includes distance to controls and placement)

that all the hardware involved in effecting the switchover was functioning properly (instruments, valves, controls, etc). No recovery analysis was performed for manual activation after failure of automatic actuation. This analysis was omitted because the affected accident sequences have frequencies less than 2×10^{-7} per reactor-year with the failure probability for basic event RA7 set to 1.0.

The probability of a Low Level alarm occurring in conjunction with a group of other alarms was addressed, as such an event could interfere with the timely beginning of the switchover procedure. On the other hand, no credit was taken for recovery from non-functioning motor operated valves ("sticking valves"), as such an eventuality would require recourse to other procedures. (The time available for carrying out the manual switchover would be exceeded, as the minimum time required to correct a sticking valve was estimated to be five to ten minutes).

6.4 Simulator Visit

The HRA team visited the Representative Plant simulator on 14 August 1992. The purpose was to begin a task analysis of the actions involved in the changeover from the injection mode to the recirculation mode following a LOCA. The task analysis began with a talk-through of the procedures, observation of a team in training performing the procedures, discussions with the instructors and team members, gathering of documents, and taking photographs of the simulator layout. Subsequently, a number of telephone conversations were held with the instructors and other staff members to gather additional information.

During the visit, the analysts observed a team-in-training perform the exercise of switchover from Injection to Recirculation for the plant operating in the semiautomatic mode. According to the instructors, thirteen minutes are allowed for the switchover, and the team under observation completed the switchover in 9 minutes. Note that thirteen minutes is an operational goal.

At the time of the visit the simulator was set up for the semiautomatic switchover mode. Therefore, the team did not observe the exact procedures followed in the manual mode, but the differences in operational requirements are few, and can be derived from the EOPs. The switchover procedures are presented in two different sets of EOPs. Both

sets are named LOCA 3, but one set applies to Unit 1 and the other set applies to Unit 2. Unit 1 uses the manual switchover mode, while Unit 2 uses the semiautomatic mode. The EOPs are marked with their respective unit numbers. The errors or failures that would affect performance during a switchover are failures of the operators to respond to alarms, errors in operating controls, errors in reading displays, or incorrect use of procedures.

6.5 Performance Shaping Factors

6.5.1 Controls and Displays

Most of the controls at the Representative Plant are transilluminated switches, called "bezels." Almost all Motor Operated Valves (MOVs) are operated by bezels, with the valve designation printed on the bezel. Separate, vertically juxtaposed bezels are used to change a valve from one state to the other. The backlighting is either red or green, to indicate the status of the valve (red for open, green for closed). Normally, one of the two bezels for a valve will be lit, indicating status. To change the state of a valve, the dark bezel is pressed. The bezel that was lit will go out, and the other bezel will light when the valve reaches the opposite state. An experienced operator knows how long it should take for the valve to "stroke," usually about 10 seconds. If the opposite bezel doesn't light within the expected time, the operator will interpret this as an indication of a sticking valve, and an Equipment Operator will be sent to complete the valve stroke manually. The indications of the bezels are controlled by limit switches mounted on the valves, so that the appropriate bezel will light when manual operation of the valve has been completed. The bezels for valves that are usually operated jointly are adjacent to each other, and can be depressed with two fingers of one hand, so that dependence between the operation of the pair of valves may be regarded as complete, (Complete Dependence, CD, as defined in the HRA Handbook).

The bezels controlling pumps are also arranged in vertically juxtaposed pairs, with the red bezel indicating "start" and the green bezel indicating "stop". When pump controls are activated the change in status is indicated immediately. The adjacent ammeter displays provide additional status feedback.

The convention is that for each pair of controls, "OPEN" is above "CLOSE", and "START" is above "STOP". When attending to the color coding, in each pair of bezels RED is above GREEN. This convention facilitates status checking.

Not every bezel is a control bezel. Many of the bezels are monitors only, to indicate status of a component or system. The labeling of the bezels indicates the subsystem of which it is a part, e.g., the letters "RH" in the label indicate that it is part of the Residual Heat Removal system, "SJ" refers to Safety Injection, "CCW" refers to Component Cooling Water, etc.

The controls for the subsystems are arranged in groups on individual panels, with the name of the subsystem above each panel, e.g., "RESIDUAL HEAT REMOVAL SYSTEM", "SERVICE WATER SYSTEM", etc. The first line below the subsystem name may list additional divisions of the subsystem; for example, on one of the panels for the RESIDUAL HEAT REMOVAL SYSTEM the second line is divided into three sections, marked RHR PUMPS, PUMP SUCTION VALVES, and COMMON SUCTION VALVES. Below these subtitles, the bezels are arranged in columns, with a list of the bezel controls immediately above each column. If more than one set of controls are in a column, the heading above the column indicates the positions of the sets of controls, by listing their designations in accord with their positions in the column.

If an operator is uncertain about the location of a specific control, he can go to the panel, find the subdivision (if required), then read across the next line to find the number of the control he wants to operate. In addition to the bezel type controls, there are some other type switches, such as the two-position override switches in the array of "ECCS POWER L/O SWITCHES", which are grouped on the rear wall. These switches are mounted on individual subpanels which light up brightly when activated. The lighted panels are easily seen across the room, so that if a switch is missed it is obvious, as it may be the only one in a group that is not lit.

Most of the quantitative displays are arranged in the subsystem groupings that they monitor. There are many vertical-scale analog displays, most of which are dual, the vertical scale providing an analog indication, with a digital indication above the scale, so that the operator can use the analog scale for

"check-reading", and the digital indicator for reading exact values. In addition to the displays used directly in conjunction with operating procedures, there is a large mimic of the "Reactor Protection Status Train" on the rear wall, which displays the status of important valves in their lineup. The mimic is in easy view of anyone in the control room.

6.5.2 Lighting

The illumination in the simulator is comfortable, and one can easily read printed instructions and all the indicators in the room. A minor problem arises with reading some of the bezels: because of position, some of the bezels are difficult to read when they are not lit because of the overhead lighting. The operators seem to have no problems with this, as they have learned to cup their hands around the problem bezels and then are able to read them easily.

6.5.3 Training

All operators at the Representative Plant units undergo eight weeks of training annually, in four sessions of two weeks each. Typically, a maximum of ten weeks elapses between training sessions. Teams are not always "intact" in the training sessions, due to absences for various causes (vacation, etc). Thus, an operating team may consist of members who have undergone retraining at different times, but none of them will have been out of training for more than 10 weeks.

Training is conducted at the Nuclear Training Center, and consists of classroom training coordinated with simulator exercises. A number of emergency procedures are presented in the classroom sessions, and the trainees do not know which of these they will be tested on in the simulator trials.

Not every possible emergency is covered in every training session, but every possible emergency is exercised at least once a year by every operator. In particular, from inquires it was learned that the manual switchover is exercised at least once annually. The simulator is modified by disabling the semiautomatic mode, so that it simulates the unit that uses the manual switchover. All operators, from both units, undergo the manual switchover training. To date, there have been no errors noted during training.

In some other plants there have been problems of cross-training operators because the control panels for two units were mirror-images of each other, i.e., a control on the right end of a panel in one unit would be on the left end of the corresponding panel in the other unit. This created an opportunity for error if an operator who normally worked in Unit A happened to be on duty in Unit B when an emergency arose, as the operator might revert to his stereotypical behavior under the stress of an emergency, and would lose time in locating essential controls or displays. This problem does not exist at the Representative Plant, as the two control rooms have identical layouts.

Simulator fidelity is an important consideration in training. In conjunction with this HRA we observed a team-in-training perform the manual switchover exercise. The operators were queried and they responded that the simulator is a very realistic duplicate of the control rooms, the only unrealistic aspect of the simulator being that "valves did not stick" in the simulator.

6.5.4 Procedures

The EOPs are of the type known as "symptom oriented." The Representative Plant EOPs are prepared like a series of flow-charts, requiring the user to follow one path. They resemble a set of logic diagrams, unambiguously indicating the action to be taken in a step-by-step manner. Throughout the action sequence, status checks of different subsystems are required by the EOP. At each check, the EOP lists the possible alternative reactions that may have occurred, and specifies the actions required for each case. Following the procedures requires no more than skill-based behavior of the team, i.e., knowledge of the location of the displays and controls. All of the action steps involve rule-based behavior.

Most of the action steps in the EOPs call for a single action, or a highly dependent pair of actions. However, there are a few instances in which the EOPs combine more than one instruction in one step, with only one check-space for the step. In such cases, the Nuclear Shift Supervisor (NSS) calls the instructions to the operator one item at a time, with

the Reactor Operator (RO) reporting the completion of each item before the NSS reads the next instruction. The NSS waits until the last item has been reported before checking the step as complete.

This symptom-oriented type of EOP is easy to follow, is intended to anticipate all probable variables, and gives the user a chance to anticipate the results of each instruction.

The EOPs are designed to cover different phases of activity following a LOCA, and are numbered accordingly. For example, EOP-LOCA-1 covers the period from the onset of a LOCA through the onset of the RWST Low-Level Alarm. When the alarm sounds, the user is directed to EOP-LOCA-3, which covers the switchover from the injection to the recirculation mode of the ECCS. This HRA is addressed primarily to the actions required in EOP-LOCA-3.

One problem that has occasionally occurred in procedures is that the people preparing them may inadvertently incorporate errors. Such a criticism would apply to any type of procedure. Procedure number AD-44 (described below) spells out a very detailed Verification and Validation program. The operators were asked if procedures are ever modified on an ad hoc basis, using hand-written notes on the procedures. They gave assurance that this does not happen. In addition to the Validation and Verification program, the EOPs at the Representative Plant are thoroughly tested through their continual use in the simulator, and any errors would show up in the course of the training exercises. The Representative Plant has prepared a guide, Procedure Number AD-44, "Emergency/Abnormal Procedures Program", which describes in great detail the preparation, validation, and use of procedures. A brief section of AD-44, describing the use of EOPs, is reproduced here:

6.2.1 All Immediate actions, except the tables, are required to be committed to memory. All Subsequent Actions are to be communicated by another individual, typically the NSS, who is reading directly from the EOP.

6.2.3 When performing an EOP, all steps will be followed in proper sequence.

6.2.4 During EOP operations, the following personnel responsibilities are in effect:

A. SENIOR NUCLEAR SHIFT SUPERVISOR (SNSS) Performs the duties of Emergency Coordinator until relieved by the Emergency Duty Officer

B. NUCLEAR SHIFT SUPERVISOR (NSS) Assumes the Control Room Command Function and reads the EOP to the Control Room Team

C. SHIFT TECHNICAL ADVISOR (STA) Monitors the Continuous Action Summaries and Critical Safety Function Status Trees.

6.2.6 All communications shall be clear, precise and conducted in a formal and professional manner. Repeat backs shall be utilized when directing individuals to perform a specific task. The NSS shall be satisfied, through repeat back, that the initial message was understood adequately.

6.2.7 The EOP, when in use, shall be utilized as part of the Control Room Narrative Log and as such shall be marked in a manner to allow for re-creation of the event. This shall be accomplished by writing on the procedure information pertaining to major evolutions or steps. This information shall include, but not be limited to, the following:

A. The time major steps were completed. Incomplete steps shall be circled. When circled steps are completed, they shall be X'd out and the time of completion entered next to the step.

B. The time and title of procedures during transitions with the EOP network.

C. The time, and if applicable, the reason for initiating and resetting of Safeguards, the stopping or starting of Safety Related and/or major pieces of equipment.

Overall, the procedures are well designed and easy to follow. The stipulation that the EOP will be used as a log, with time entries for all major steps, provides very high motivation for the user to follow the EOP as prescribed (Step 6.2.7).

In the course of an accident, the NSS reads an instruction from the EOP to an RO, and the RO

repeats the instruction, to indicate that he has understood it. He then performs the task, let us say, closing a valve. The RO waits until he gets the indication that the valve has closed, and then informs the NSS that the task is done, and the NSS checks off the completion of the task on his EOP sheet. This system provides a very positive arrangement to ensure the timely performance of all steps required by the EOP.

NOTE: Throughout this text, reference to "the RO" implies the primary operator (or board operator), the one carrying out the instructions called out by the NSS.

6.5.5 Dependence

In estimating Human Error Probabilities (HEPs), the extent of dependence, or "coupling", between personnel and between tasks must be considered. Dependence is an important factor in estimating HEPs when developing overall estimates of team errors.

The HRA Handbook describes five levels of dependence, ranging from zero dependence (ZD) to complete dependence (CD). ZD implies that there is no interaction between the error probabilities of people, i.e., the HEP of one person is unaffected by the HEP of a co-worker.

Actually, ZD is rare among team members, as they know each other's capabilities under normal circumstances, and tend to rely on each other. Thus, if person A commits an error while person B is observing him, person B is less likely to notice the error, because B has developed an expectancy that A will perform his tasks correctly.

There were no means of objectively measuring dependence between people, but it was necessary to make estimates. The operating procedures that were observed will be described briefly, and then the estimates of dependence will be presented.

In case of an emergency, a minimum of four people will be in the Control Room: the NSS, one Senior Reactor Operator (SRO), one RO, and the STA. The NSS will be at the control position with the EOPs, and the STA will also have a set of EOPs. Typically, the NSS reads an instruction aloud to the RO, who carries out the task and reports back. The NSS then checks off the step on his EOP and proceeds to the next step.

Both the NSS and the SRO are checking the work of the RO, but they are not independent of the RO. There is dependence between each of the supervisors and the RO, due to their familiarity with him and their knowledge that he usually does his job correctly. A high dependence (HD) was assumed between the SRO and the RO, and moderate dependence (MD) between the NSS and the RO. For the situation described, the error probability of the SRO is 0.5, and of the NSS it is 0.15, with error factors of 3 (Table 20-21 of Swain and Guttmann). However, although most of the operator actions take place within view of the NSS, he is not close enough to read the bezels, even though he can usually ascertain whether the correct bezel was activated. For this reason checking error probability of the NSS was arbitrarily doubled to 0.3. The error probability of 0.3 allows for those instances in which the NSS may be briefly distracted from observing the RO.

The SRO is able to move freely and observe the RO at close range, so his checking HEP of 0.5 does not require modification. As with the NSS, the HEP of 0.5 allows for instances in which the SRO may be briefly distracted from observing the RO. Note that credit was not allowed for the effects of additional operators, even though there will be additional operators in the control room, who will provide additional checking on the primary RO. (When the NSS calls instructions to the RO, he can be heard by everyone in the control room). Similarly, no recovery factor was allowed for the presence of the STA, since he normally is not observing the operator actions.

6.5.6 Levels of Behavior

One of the considerations in assessing human reliability is the level of behavior involved in carrying out a task. Traditionally, Human Reliability Analyses have considered three levels of behavior: Rule-based, Skill-Based, and Knowledge-based. Rule-based behavior is involved when a person follows a procedure in a step-by-step manner, without requiring extensive knowledge of the system. Skill-based behavior is involved when a person engages in behavior that is "second nature" as the result of extensive training and practice, e.g.,

scramming the reactor when a turbine-trip occurs. Knowledge-based behavior is involved when a person has to engage in reasoning, e.g., diagnosing the cause of an unexpected event. This process is also called "decision-making".

In this HRA, rule-based behavior is exemplified by the process of the NSS reading instructions from the EOPs to the RO, and the RO carrying out the instructions. The instructions are called out one at a time, so that the entire procedure is carried out in a step-by-step manner. Most of the HEPs in this HRA are based on the performance of such rule-based behavior.

Skill-based behavior is exemplified by the team members' knowledge of the "geography" of the Control Room. It was assumed that all the operators are thoroughly familiar with the locations of all the controls and displays, and that the RO can go directly to each subpanel for each equipment group as instructions are called by the NSS.

Knowledge-based behavior is difficult to quantify, and is much more subject to degradation under the effects of stress. An example of knowledge-based behavior would be the decision required when a recovery-factor indicates that some previous step in the procedures was not carried out. The operating team must decide which step had been omitted and take corrective action. Although the answer may be obvious to the highly trained operators, they do involve some decision-making.

6.5.7 Stress

Stress is a word that is used loosely in everyday conversation, and has often been defined loosely. The definition of stress used in the present study is "Bodily or mental tension, ranging from a minimal state of arousal to a feeling of threat to one's well-being, requiring action." Although the degree of stress is a continuum, for HRA we use four levels: Very Low, Optimum, Moderately High and Extremely High. Optimum stress is the comfortable, facilitative level associated with normal task-loads. Extremely high stress is induced by a situation that threatens a person. Threat stress was assumed to develop when a LOCA or similar serious accident occurs, and to prevail until the operating team "gets a handle on it", and begins to get control of the situation. This implies that the extremely high level of stress exists during the initial decision-making period, when the team realizes the existence and nature of the accident, through the early period of initiating corrective action. Threat stress can be very disruptive of behavior, and reduces human reliability greatly.

Moderately high stress is associated with heavy task-loads, such as would exist when the operating team is carrying out the ECCS switchover following a LOCA. At Unit 1 of the Representative Plant, it is a goal that manual switchover will be accomplished in only 13 minutes. The team-in-training completed the task in 9 minutes, which was about average time in simulator exercises. In a real emergency the team would be under higher stress, and would be more likely to commit errors. It was reasoned that the team would no longer be under threat stress because the accident has been diagnosed and is under control, but the plant would still in danger and the switchover must be accomplished promptly.

6.5.8 Levels of LOCA

The EOPs are identical for all 3 levels of LOCA, small, medium and large, so the only difference in performance under the 3 levels of LOCA might be due to different levels of stress with time. The operators are trained to execute the entire procedure within the time available in the worst case; they are not trained to take more time for a smaller break. Stress levels might abate sooner following a small LOCA than after a large LOCA. However, this is difficult to assess, and the same stress level was assumed during switchover regardless of the level of LOCA. Because both the pace of the operation and the prospects for recovery are largely independent of the level of LOCA, this HRA calculated all failure probabilities except diagnosis under the assumption that a large LOCA has occurred.

6.6 Summary of Performance Shaping Factors

The above description of the relevant PSFs indicates that, with the exception of Stress, all the PSFs are very favorable, and suggests that we could modify the tabled nominal HEPs downward. For the sake of conservatism we used the unmodified HEPs. The high stress level increases all error probabilities.

The procedures are written such that almost all actions are carried out in a step-by-step manner (rule-based behavior). This situation applies to the NSS as well as the RO. In such cases, the HRA Handbook recommends that the nominal HEPs be multiplied by a factor of 2 (Table 16, item 4). With a few exceptions, this approach was applied, using the nominal HEPs from the tables, and doubling their values to allow for the effects of stress.

6.7 Items of Interest in the HRA

The errors or failures that would affect performance during a switchover are failure to recognize that a LOCA is in progress, failures of the team to respond to alarms, errors in operating controls, errors in reading displays, and errors of omission.

6.7.1 Errors of Omission

Customarily, HRAs address both errors of commission and errors of omission in evaluating human reliability. In the Representative Plant switchover analysis, errors of omission by ROs were not considered to be a significant probability because of the regimen followed. The NSS calls the instruction to the RO, who repeats it to indicate that he has understood the instruction. The RO immediately applies himself to the task, and upon completing the task, informs the NSS, who checks it off on his EOP. None of the actions required of the RO are complex; most of the instructions involve the operation of a valve or pump, or verification of status lamps. Despite the stress that the team is under, the task requirements are modest. There is no requirement for the RO to memorize a series of instructions.

In addition to the discipline inherent in the above procedure, we have the positive effects of human redundancy, in that both the SRO and the NSS (and possibly other ROs) are observing the RO as he carries out his tasks. Barring some major distraction, the probability that the RO would fail to carry out a specified act is negligible, and was disregarded in the analysis.

There is a possibility that the NSS might omit a step as he is reading instructions to the RO. The HRA Handbook (Swain and Guttmann) lists a probability of 0.003 (EF=3) for omission of an item when using a long list (more than 10 items), even when checkoff is required. However, the HRA Handbook table was intended for the conventional checklist such as is used when carrying out maintenance procedures. When using such checklists it is very easy to violate good practice and to check off a group of steps at a time, thus possibly checking an item that was not performed.

The EOPs are not typical checklists; they are flow-charts with decision steps and action steps in sequence. Also, there are Notes and Cautions in the flow-path. The decision steps, notes, and cautions are very distinctive, in that they are in larger and different formats from the rectangles used for action steps, and they are unlikely to be missed by the user. Typically, the decision steps, notes and cautions direct the user's attention to the immediately following action step. Also, the NSS "keeps his place" on the EOP with his finger, and records the time of completion of major steps. Still, under stress, there is a small probability that the NSS might skip a step as the result of some distraction. Although the NSS is working in a dynamic situation, reading the instructions from the EOP is a step-by-step task, and an HEP of 0.002 was assigned to the probability of skipping an action step in the EOP. This is the lower bound of the tabled HEP (nominally 0.003, raised to 0.006 to allow for the effects of stress). The lower bound was used because of the excellence of the written procedure and the disciplined manner of use required by the Representative Plant Procedure Number AD-44.

In the EOPs the Notes and the Decision diamonds are so distinct that a minimal value of 0.001 was assigned to the probability of failing to notice one of them. Also, the step immediately following one of these items was similarly given a minimal probability of omission, because the distinctive item usually directs the user to the immediately following step.

6.7.2 Errors of Commission

Errors of commission in carrying out action steps are quantified in accord with HRA Handbook tables (Swain and Guttmann) on the basis of the task analysis. The HEPs are modified to consider the effects of stress, PSFs, and other factors, such as the recovery potential resulting from human

redundancy and from mechanical recovery factors inherent in the power plant system.

Most of the RO actions in the control room involve selection and activation of a control, usually a bezel. A bezel is a novel device, in that it combines both the display and the control in one element. Thus, for the operator, selection and activation are a single act; the RO literally "puts his finger on it" to accomplish both selection and activation. When errors of commission for the RO are listed only one error term is used, the term for selection. Similarly, when the RO is required to verify status by referring to a bezel, only the error of selection is considered, as the probability of misinterpreting status is negligible.

In most cases in which a selection error is possible, there are one or more alternate controls that the operator could select. These alternate controls are described in the text for each event, as an aid in determining recovery factors. When there are no plausible alternates, the failure limb would usually be quantified as negligible. Even with conservatism, errors of commission would have a negligible contribution.

6.8 Assumptions

The following assumptions are made in estimating the error probabilities in carrying out a switchover from injection to recirculation mode at the Representative Plant.

1. A large-break LOCA has occurred, the ECCS is operating in injection mode, and the RWST is approaching low level. At this time the plant is beyond the stage at which an "incredulity response" would interfere with corrective actions, but the staff are still experiencing moderate stress. The highest level of stress, threat stress, would be assumed for the initial realization of a large-break LOCA, but by the time switchover to recirculation is needed, the situation is understood and under control. Moderately high stress was assumed because the plant is still in danger, and prompt actions are required to keep it safe.

2. The staff consists of a STA, a NSS, a SRO, two ROs, and two Equipment Operators (EOs). Equipment Operators are trainees who are not as yet licensed operators, but who are authorized to manipulate valves and other controls. It was assumed that all the licensed operators have more than six months experience, (i.e., they are not novices). The STA may or may not be a licensed operator; his specific functions are Monitoring the Continuous Action Summaries and Critical Safety Function Status Trees. The STA is responsible for communicating overall plant status to the NSS. For the purpose of this study, the STA was not considered as a recovery factor in the step-by-step activities involved in following the EOPs.

3. The NSS is using the EOPs in accord with plant administrative policies. Many of the action steps can be completed promptly as they are called to the RO, and can be checked off on the EOP as the RO notifies the NSS that the action is complete. If an action is initiated but not completed before initiation of the subsequent step, the NSS circles the step to indicate that it is in progress. When the action is completed, he places an "X" on the circled step and the time of completion is logged. Adherence to this policy is crucial to the validity of the HRA, and there is a compelling rationale to believe that the policy will be followed. First, the EOPs are well designed, easy to follow, and the markings provide the NSS with a continuous record of what has been done and "where he is" in the recovery process. Second, the plant policy is that the marked EOP will serve as a log of the actions that took place during the emergency. Thus, the marked EOP provides administrative protection for the operating team in case of any subsequent inquiries, which serves as a very high motivation to use the EOPs in accord with plant policy.

As observed in the simulator, the NSS is positioned at a desk from which he can view most of the control room, with the EOP in front of him. From his position the NSS can observe most of the operator activities, and can tell the status of most of the bezels (status is indicated by color). The SRO also acts as a monitor of the RO. All team members can hear the instructions being called out by the NSS and are alert for the possibility of errors. In

addition to the NSS, the STA has a copy of the EOP and continuously monitors plant status.

6.9 Quantitative Results for EOP Steps

This section provides an evaluation of each step of the switchover process, beginning with diagnosis and startup. Each relevant step of the EOP is discussed separately. In this analysis HEPs from the HRA Handbook (Swain and Guttmann) were used, and the appropriate tables in the HRA Handbook are referenced. Before quantifying the HRA, every action step was evaluated individually, including steps that are not covered by the model in Section 5. Each of these steps was evaluated to determine whether failure to perform the step correctly would have a significant probability of causing switchover failure. It was found that each of these additional steps can be omitted from the analysis because it has one of the following attributes:

- it is not relevant to the success of ECCS switchover;
- it would already have been completed during performance of a previous EOP or the LOCA;
- it permits recovery from an equipment failure, but the Sequoyah PRA takes no credit for the recovery; or
- it reconfigures the ECCS system to protect against later failure of a component.

In quantifying each step, the following method was used: the potential error of omission by the NSS is evaluated for each step, and was assigned one of the two values described in the section on Errors of Omission, either 0.001 or 0.002 (EF=5). The HEP for the potential error of commission by the RO was then determined, using the appropriate tables, and this HEP was multiplied by the joint probability that neither the SRO nor the NSS will detect the error, if committed. This joint probability of failure was assumed to be constant throughout the switchover period, (9 to 13 minutes). As described in the section on Dependence, this joint HEP was 0.3 x 0.5 = 0.15.

The Commission HEP was multiplied by the Detection HEP, and added to the Omission HEP to yield the combined HEP for each step.

In the EOP some action steps are numbered in groups. To distinguish individual steps, letters were assigned to each step within each group. The first step in, say, group #9, is designated 9.a, the next is 9.b, and so on. If there was only one step to a number, no letter was assigned.

The HRA Handbook requires consideration of plant-specific factors that can affect diagnosis error probability. The symptom-oriented EOPs are designed such that the operator should not have to diagnose the event. Furthermore, the event is a well-recognized classic. The operators have practiced the event in the simulator requalification exercises. Interviews indicate that the operators have a good recognition of the relevant stimulus patterns and know which written procedures to follow.

6.9.1 Diagnosis

The first task is for the operators to recognize that a LOCA is in progress and enter the EOP LOCA 1. Estimates for diagnosis errors were based on the Sandia Recovery Model (Weston and Whitehead), with consideration of the Operator Action Tree (Hall and Fragola).

For medium and small breaks (S1 and S2), the time available for diagnosis was taken to be 20 minutes, consistent with the NUREG-1150 analysis (Bertucio and Brown). For very small breaks (S3) NUREG-1150 allows 30 minutes for diagnosis. The NUREG-1150 analysis did not have to assign a time for diagnosis of large breaks; the present study used the Representative Plant time of 14 minutes.

In the Sandia Recovery Model, the problem group that most closely approaches the small LOCA is group #1, "Probability of failure to manually operate a system or component to control a critical parameter prior to automatic actuation (if it has automatic actuation)." Data were gathered on 63 trials. The curves show a failure probability approaching zero at 20 minutes, with a 95% upper confidence bound of 0.02. Graphical interpolation to 14 minutes gave a mean of about 0.005 with an error factor of 6.

The curves could not be interpolated to longer times. Instead, the HRA Handbook was used to determine the ratios of diagnosis failure probabilities for smaller LOCAs to that for a large LOCA. This resulted in failure probabilities of 0.0015 at 20 minutes and 0.00015 at 30 minutes.

The Operator Action Tree (OAT) model indicates a diagnosis failure probability of 0.006 at 15 minutes. Both sources are in good agreement. Although the differences are negligible, the Sandia recovery model data were used because they are more recent and based on a larger number of cases.

6.9.2 Timing

The switchover begins with step 15 in EOP LOCA 1, which requires verification that at least one RHR pump is running. This step alerts the team to the subsequent activity of switching to the recirculation mode. The following step, #16, alerts them to the onset of the alarm signaling RWST LOW LEVEL. The alarm is the signal to change to EOP LOCA 3, the procedure for switchover.

Under ordinary circumstances, an annunciated alarm is so compelling that it is very unlikely to be ignored. In this situation the team is awaiting the alarm, with the STA specifically assigned to monitor the RWST level, so the probability that an operator would miss it is possibly even less than that of failing to notice a single alarm when no others are sounding (0.00001, Table 20-23, #1). At least three other people will be available to notice the alarm: the RO, the SRO, and the NSS. Allowing for the effects of dependence, the joint probability of failure to notice the alarm is 0.0000015, which is considered negligible. (The situation is much different if the Low Level alarm occurs when a group of other alarms are sounding. This is described in Section 6.10.)

Responding to the alarm, EOP-LOCA-3 is used. The first action required is the determination that the containment sump level is at 68% or above (step 4). Step 16 in EOP-LOCA-1 is a decision diamond, "Is RWST Low Level Alarm (15.24 ft) Actuated". This decision diamond is an alerting factor to the operating team that the Containment Sump Level must be monitored, as subsequent actions are contingent upon the height of the liquid in the sump. Therefore, even though it is not required by the EOPs, there is confidence that at this juncture an operator will be assigned to monitor the sump level indicators.

The sump level indication consists of two vertical scale analog displays with digital readouts above them (a two-channel system). An RO reads the indicators, and calls out the reading to the NSS. Ordinarily, a negligible HEP would be assigned to the task of reading the indicators; both analog and digital outputs are being presented. The nominal HEP for check-reading an analog indicator is 0.001 (20-11, item 2), and the HEP for reading a digital indicator is 0.001 (item 2).

Although it is not required by the EOP, observations have shown that it is common practice for operators to make some kind of mark on the analog scales to facilitate check-reading. We would expect the Representative Plant operators to prepare similar aids, such as pencil-mark or other mark at the 60% level on the analog scales. However, in the Representative Plant arrangement such added marks are not necessary, as the uppermost letter of the word "Level" coincides with the 68% level on the analog display, and is readily visible from a distance of several feet.

Such aids are intended to alert the RO to the rising sump level. For exact values they refer to the digital readouts immediately above the analog scales.

In accord with our stress model, the error probabilities were doubled for each action, yielding an HEP of 0.002 for failing to note the analog indication and 0.002 for misreading the digital indication. Although there are two sets of displays available to the RO, there is a tendency for an RO to "funnel" his attention in cases such as this, and to focus on only one set of displays.

The probability that the RO would misread both indications in a single set of displays is 0.002 times 0.5 (a high dependence was assumed between the RO and his own errors - if he makes an error on one action he is likely to make a similar error on the immediately subsequent action). The recovery factor exists in the probability that one of the other operators will notice the error (for example, the SRO). Because the SRO has high dependence with the RO his probability of failure to detect that the 68% level has been reached is also 0.5. Thus, the

joint probability of failure was calculated to be 0.002 x 0.5 x 0.5 = 0.0005 (EF=10).

Step #4b (semiautomatic only)

Depress SUMP AUTO ARMED push buttons on 21 and 22 SJ44 bezels.

These push buttons are the topmost in two adjacent columns of bezels. There are no other bezels next to them. The minimal selection error of 0.001 was assigned to the pair. Complete dependence was assumed because of the wording of the instruction and the physical arrangement of the pair; the RO would press both of them simultaneously. The commission error is 0.001 x 0.15 = 0.00015. On the EOP this action step immediately follows a decision diamond, so the error of omission is 0.001. The combined HEP = 0.001 + 0.00015 = 0.00115.

Step #6

Remove the following lockouts at 1RP4

2SJ30 (from RWST)
2SJ69 (common suction)
2SJ68 (SI Pumps Miniflow)
2SJ67 (SI Pumps Miniflow)

The above lockouts are switches on the back panel next to the Safeguards Status display.

The reliability of this step depends upon the physical arrangement of the switches, the way they are marked, and on the attentiveness of the person checking the performance of the operator manipulating the switches.

It must be noted that the removal of a lockout is a very special type of activity for operating team members. Lockouts are part of the plant safety system, which prevent inadvertent operation of certain critical components. Operators are trained to regard the lockouts as sacrosanct, and to be extremely cautious if required to remove them. ("Removal" of a lockout involves closing a switch to complete the circuit between the primary control switch and the controlled element.) Because of their training, operators are inordinately careful in carrying out this task. Also, the human monitor, (the SRO) will be inordinately alert in verifying the RO's selection, not only because of the attitude toward lockouts, but because in this particular situation he is the sole monitor, as the lockout panel is not in view of the NSS.

The four lockout switches are part of a group of 21 switches. The four switches are not a single group, but they are very clearly marked with both text and numerals. The nominal HEP for selection is 0.003, doubled for stress = 0.006, with an error factor (EF) of 3, (Table 20-12, #2). Because of the unusual concern attached to this task, the nominal HEP, 0.003 was used. Also, for this one task, the SRO's high level of dependence was disregarded and this task was treated as a special, short term, one-of-a-kind checking with alerting factors, with an HEP of 0.05 (Table 20-22, #3).

As outlined in the section on Errors of Omission, consideration had to be given to the NSS's probability of omitting a step when calling instructions to the RO. In this step the written instructions are presented in an unusually large and very distinctive "box", so we use the lower HEP for Omission, 0.001. The error probability for any single one of the four switches is the omission HEP added to the joint HEP for error by the RO (0.003) and failure of the SRO to detect and recover the error (0.05).

The combined HEP, per switch, was calculated to be 0.001 + (0.003 x 0.05) = 0.001 + 0.00015 = 0.00115, with an EF of 5 (20-20, #4).

NOTE: There are partial recovery factors for errors in this step in subsequent steps 9.1i and 11, which require closure of the valves controlled by the lockouts. For example, assume an error on just one of the lockout switches. If the RO were unable to achieve closure when required, he might assume a sticking valve, but he might also consider a failure of the lockout removal and recheck the status of the lockout.

The dominant error factor in the above HEPs is the error of omission. If it is assumed that the omission error occurred, none of the lockouts would be removed, and the RO would notice this quickly in step 9.1i, because neither valve would close. Because the EOPs specifically enjoin the operator from pausing to correct malfunctions, no credit was taken for the possible recovery in steps 9.1i and 11.

Step #9.1b (manual only)

Stop the following pumps
21RHR pump
22RHR pump
21 or 22 CS pump - (not quantified here)

The bezels for the two RHR pumps are the bottom pair in two adjacent columns, and they are the only STOP bezels. Because of their distinctive location, a minimal selection error of 0.001, was assigned and doubled for stress (0.002). There is a recovery factor in the immediate feedback from the pump ammeters. An HEP of 0.2 was arbitrarily assigned for failure to observe the ammeters. The joint HEP per switch was calculated to be 0.001 for omission (this action step is immediately below a note) plus 0.002 x 0.2 x 0.15, i.e., 0.001 + 0.00006 = 0.00106.

Step #9.1c (manual only)

Open CCW to RHR HX Outlet Valves 21 and 22 CC16

Because of their arrangement, a selection error of 0.002 was assigned to these bezels. However, this error applies to both bezels jointly, as they are next to each other. In this situation complete dependence was assumed, because of the nature of the instructions, the physical arrangement of the bezels, and the obvious manner in which they will be operated (both at once). The omission error was 0.002 added to the commission error of 0.002, which was multiplied by the checking error of 0.15. The HEP for this step was calculated to be 0.002 + 0.0003 = 0.0023.

Step #9.1d (manual only)

Close Pump Suction Valves 21 and 22 RH4

This step is similar to step #9.1c, and the same rationale applies. The HEP for this step is 0.0023. Complete dependence was assumed.

Step #9.1f (manual only)

Open Sump Valves 21 and 22 SJ44

The rationale is similar to that in the above steps, except that this step directly follows a note, so the omission error is 0.001.

The HEP for this step is 0.0013.

NOTE: There are positive recovery factors for the opening of these valves in Notes 9.2 and 9.3. Applying the recovery factors, the HEP for this step becomes insignificant.

Step #9.1h (manual only)

Start 21 and 22 RHR Pumps

These are the only bezels that can be activated when the pumps are off. The minimal HEP of 0.001 applies. The instructions, physical arrangement, and obvious mode of operation indicate complete dependence between the two pumps (if the RO starts either, he starts both). Omission error is 0.002, added to 0.001 x 0.15, i.e., 0.00215, the HEP for this step.

Step #9.1i (manual)

Step #9.1k (semiautomatic)

Close SI Pumps Miniflow Valves 2SJ67 and 2SJ68

The controls for the miniflow valves are in a subgroup at the bottom of a double column. The two bottom bezels are the CLOSE controls, and the only ones that can be activated. The minimal HEP of 0.001 applies for selection. The calculations are the same as in step #9.1h. The HEP is 0.00215 for this step.

NOTE: Note 9.2a provides a recovery factor, as it requires that the status of these valves be checked. If the recovery factor is applied, the HEP for this step becomes insignificant.

Step #9.2a

This is a Note requiring verification of
22SJ44 Open
2RH1 or 2RH2 Closed (not quantified in this HRA)
2SJ67 or 2SJ68 Closed

For 22SJ44 use selection error of 0.002. Omission error is 0.001 (this is a Note). The checking error is 0.15. Joint HEP for 22SJ44 is 0.0013.

For 2SJ67 and 2SJ68 the selection error is 0.001. The two bezels are side by side, if the RO sees either he sees both, so the joint HEP for the pair of valves is 0.001 (omission) plus 0.001 x 0.15, i.e., 0.00115.

Step #9.2b

Is Common Suction Valve 2RH1 or 2RH2 Closed

This is a decision diamond, so the omission error is 0.001. The bezels are the bottom bezels in the Common Suction Valve sub-panel. Assign a selection error of 0.002 for the pair (if RO sees either he sees both). The joint HEP for verification of the pair of bezels is 0.0013.

Step #9.2c

Open RHR Discharge to Charging Pumps Valve 22SJ45

In the manual procedure, omission error is 0.001, as this step is immediately below a decision diamond. Selection error is 0.002, checking HEP is 0.15. The joint HEP for this step is 0.0013.

For the semiautomatic procedure, the omission error is 0.002, and the Joint HEP is 0.0023.

Step #9.3

This is a Note, similar to step #9.2a, except that RO checks 21SJ44 instead of 22SJ44. The HEPs are the same for both Notes:

HEP for 21SJ44 = 0.0013.
HEP for the pair of valves, 2SJ67, 2SJ68 = 0.00115.

Step #9.4a

Open RHR Discharge to SI Pumps Valve 21SJ45

This is similar to step #9.2c. In the manual procedure, this step immediately follows a note, so the omission error is 0.001. Selection error is 0.002, checking HEP is 0.15. Joint HEP for this step is 0.0013.

For semiautomatic, the Joint HEP is 0.0023.

Step #9.4b (manual only)

Open SI-CHG Pumps X-OVER Valves 21 and 22SJ113

These bezels are the center pair in a subgroup of six X-OVER bezels. Selection error is minimal, 0.001, as there are no credible alternate bezels to select. The omission error is 0.002. The instructions, physical arrangement, and obvious mode of operation indicate complete dependence (if RO actuates either bezel, he will actuate both). Checking HEP is 0.15. Joint HEP for the pair of bezels is 0.00215.

Step #11

Close the following valves
2SJ30 (from RWST)
2SJ1 (RWST to CHG Pump)
2SJ2 (RWST to CHG Pump)
2SJ69 (Common Suction)

Bezels 2SJ30 and 2SJ69 are very easily found, both are the bottom bezels in the only pair of bezels at the bottoms of otherwise empty columns. For each of these bezels the selection HEP is the minimum, 0.001. This action step is written in an oversized action "box," so the omission HEP for each item in the box is 0.001. Checking HEP is 0.15. For these actions the JHEP is 0.00115 each. Similarly, the operations of bezels 2SJ1 and 2SJ2 have a JHEP of 0.00115 each.

The EOP contains the caution, "Changeover to Cold Leg recirculation must be done quickly. Complete the transfer sequence before correcting valve or pump malfunctions." Another caution states, "IF at least one flow path from the recirculation sump to the RCS cannot be established or maintained, THEN go to EOP-LOCA-5, 'Loss of Emergency Recirculation.'" As a consequence, this HRA takes no credit for any recovery action unless it is specified in detail by the procedure. In particular, the probability of recovery is independent of the level of LOCA.

6.10 Response to Annunciated Alarms When Several Are On At One Time

In Section 6.9 reference was made to the possibility of failing to respond to an annunciated alarm when more than one alarm, or group of alarms, was sounding at once. As a hypothetical case, assume that something goes amiss, distracting the STA at about the time that the RWST Low-level alarm is ready to sound, and that five alarms are demanding attention when the Low-level alarm sounds. Thus, the Low-level alarm is the sixth alarm to sound. Table 20-23, line 6, indicates a basic HEP of 0.016 (EF=10) for such a situation. This is premised on the assumption that the team is very highly overloaded, and the sixth alarm to sound is "just one more", and may not be attended to promptly. Of course, human redundancy is available to ameliorate this situation. The SRO still has an HEP of 0.5, and the HEP for the NSS is 0.15 (it is no longer doubled to 0.3, as the annunciators are read more easily than are the bezels). Thus, the basic HEP of 0.016 is multiplied by 0.075, to yield a joint HEP of 0.0012, which is significantly higher than the HEP for a single annunciator.

6.11 Probabilities of Manual Switchover Control Failures

This section derives approximate probability distributions to replace the NUREG-1150 data for the events in Table 5-4. The distributions were based on the results given in Section 6.9 for individual steps of the EOP.

CW-21CC16-OP 0.0
CW-22CC16-OP 0.0
LPR-HE-FO-CHR 0.0023 (EF=3)
The analysis of Step #9.1c assumed complete dependence in opening 1CC16 and 2CC16. The error factor was determined by the dominant contribution, the omission error.

HP-21SJ113O-OP 0.0
HP-22SJ113O-OP 0.0
HPR-HE-FO-V6V7 0.00215 (EF=3)
Here the analysis of Step #9.4b indicates complete dependence for operating 1SJ113 and 2SJ113. As before, the omission error dominates and determines the error factor.

HP-21SJ45O-OP 0.0013 (EF=3)
HP-22SJ45O-OP 0.0013 (EF=3)
HPR-HE-V8V11 0.0
Because operations on 1SJ45 and 2SJ45 are separated, appearing at Steps #9.2c and 9.4a, the analysis assumed zero dependence. The omission error dominates and determines the error factor.

HP-2SJ1C-OP 0.00115 (EF=3)
HP-2SJ2C-OP 0.00115 (EF=3)
HPR-HE-FO-CHISL 0.0
The analysis of Step #11 assumed that errors in operating SJ1 and SJ2 have zero dependence. The error factor is that of the omission error.

HPR-HE-FO-631 0.0023 (EF=4)
HPR-HE-FO-635 0.0023 (EF=4)
Failure to operate SJ30 or SJ69 may occur from an error in removing a lockout (Step #6) or an error in operating the bezel (Step #11). Because the EOP instructs the SRO to complete the procedure before correcting valve malfunctions, no credit was taken for recovery at Step #11 from an error at Step #6. The error factor is a combination of an EF of 5 for Step #6 and an EF of 3 for Step #11.

HPR-HE-FO-SIMIN 0.001 (EF=3)
HPR-HE-FO-SIMN1 0.001 (EF=3)
HPR-HE-FO-SIMN2 0.001 (EF=3)
LPR-ICC-NO-63175 0.00015 (EF=3)
LPR-ICC-NO-633 0.00015 (EF=3)
LPR-ICC-NO-634 0.00015 (EF=3)
It was assumed that SJ67X would be included in Step #6 if there were such a valve in the system. The analysis of Step #6 indicates that the error of omission may be completely dependent for removing lockouts on SJ67, SJ68, and SJ67X. For the error of commission, this analysis assumed zero dependence. There is also the possibility of error at Step #9.1i; but the recovery at Step #9.2a reduces the probability to 2.5×10^{-6}, which is negligible in comparison to the Step #6 probabilities.

L3-RWSTL-OP1 (AH1) 0.0062 (EF=6)
L3-RWSTL-OP (S1 or S2) 0.0027 (EF=6)
L3-RWSTL-OP2 (S3) 0.0014 (EF=10)
For failure to respond to the RWST low-level alarm, this analysis assumed the unfavorable environment of Section 6.10, in which five other alarms are already sounding. The diagnosis error is included.

LP-2122RHR-CC 0.00215 (EF=3)
LP-21RHR-OR 0.0
LP-22RHR-OR 0.0
The analysis of Step #9.1h indicated complete dependence between operator actions to restart the RHR pumps. The error factor was determined by the dominance of the omission error.

LP-2122RHR-OS 0.0
LP-21RHR-OS 0.00106 (EF=3)
LP-22RHR-OS 0.00106 (EF=3)
Because Step #9.1b lists each pump on a separate line, the analysis assumed zero dependence for stopping the RHR pumps. The error factor is that of the dominant omission error.

LP-2122SJ44-CC 0.0013 (EF=3)
LP-21SJ44O-OP 0.0
LP-22SJ44O-OP 0.0
The analysis of Step #9.1f concluded that the opening operations for 1SJ44 and 2SJ44 are completely dependent and that the omission error dominates.

LP-21RH4C-OP 0.05 (EF=2)
LP-22RH4C-OP 0.05 (EF=2)
According to the analysis of Step #9.1d, there is complete dependence in the closing of valves 21RH4 and 22RH4, with a failure probability of 0.0023 (EF=3). However, the failure model does not provide a common cause operator error for these valves. To approximate the complete dependence, the individual valve operations were assigned distributions whose product (assuming correlation) is approximately the probability distribution for coupled failures. Thus any cut set containing both failures was evaluated as though the pair was replaced by the common cause event.

LP-SUMPL-OP 0.0005 (EF=10)
The analysis of Step #4 gives the above probability distribution for misreading the sump level and unnecessarily abandoning the switchover procedure.

6.12 Probabilities of Semiautomatic Switchover Control Failures

This section derives approximate probability distributions to replace the NUREG-1150 data for the events in Table 5-4. The distributions were based on the results given in Section 6.9 for individual steps of the EOP.

HP-21SJ45O-OP 0.0023 (EF=3)
HP-22SJ45O-OP 0.0023 (EF=3)
HPR-HE-V8V11 0.0
Because operations on 1SJ45 and 2SJ45 are separated, appearing at Steps #9.2c and 9.4a, the analysis assumed zero dependence. The omission error dominates and determines the error factor.

HP-2SJ1C-OP 0.00115 (EF=3)
HP-2SJ2C-OP 0.00115 (EF=3)
HPR-HE-FO-CHISL 0.0
The analysis of Step #11 assumed that errors in operating SJ1 and SJ2 have zero dependence. The error factor is that of the omission error.

HPR-HE-FO-631 0.0023 (EF=4)
HPR-HE-FO-635 0.0023 (EF=4)
Failure to operate SJ30 or SJ69 may occur from an error in removing a lockout (Step #6) or an error in operating the bezel (Step #11). Because the EOP instructs the SRO to complete the procedure before correcting valve malfunctions, no credit was taken for recovery at Step #11 from an error at Step #6. The error factor is a combination of an EF of 5 for Step #6 and an EF of 3 for Step #11.

HPR-HE-FO-SIMIN 0.001 (EF=3)
HPR-HE-FO-SIMN1 0.001 (EF=3)
HPR-HE-FO-SIMN2 0.001 (EF=3)
LPR-ICC-NO-63175 0.00015 (EF=3)
LPR-ICC-NO-633 0.00015 (EF=3)
LPR-ICC-NO-634 0.00015 (EF=3)
It was assumed that SJ67X would be included in Step #6 if there were such a valve in the system. The analysis of Step #6 indicates that the error of omission may be completely dependent for removing lockouts on SJ67, SJ68, and SJ67X. For the error of commission, this analysis assumed zero dependence. There is also the possibility of error at Step #9.1k; but the recovery at Step #9.2a reduces the probability to 2.5×10^{-6}, which is negligible in comparison to the Step #6 probabilities.

L3-RWSTL-OP1 (AH1) 0.0062 (EF=6)
L3-RWSTL-OP (S1 or S2) 0.0027 (EF=6)
L3-RWSTL-OP2 (S3) 0.0014 (EF=10)
For failure to respond to the RWST low-level alarm, this analysis assumed the unfavorable environment of Section 6.10, in which five other alarms are already sounding. The diagnosis error is included.

LP-2122SJ44-CC **0.00115 (EF=3)**
LP-21SJ44A-OP **0.0**
LP-22SJ44A-OP **0.0**
The analysis of Step #4.b concluded that the opening operations for 1SJ44 and 2SJ44 are completely dependent and that the omission error dominates.

LP-SUMPL-OP **0.0005 (EF=10)**
The analysis of Step #4 gives the above probability distribution for misreading the sump level and unnecessarily abandoning the switchover procedure.

7.0 Calculated CDF Contributions

7.1 Method for Calculating Contributions to CDF

In this study, the CDF contribution of a failure mode or a set of failure modes is defined in terms of risk reduction. The contribution is the amount that the CDF would be reduced if all of the subject failure modes were eliminated.

The process for obtaining the uncertainty distribution for the contribution of a set of failure modes began with identifying the dominant minimal cut sets containing those modes. Then all data (frequencies or probabilities) were set to zero except for those initiators and base events that appeared in the identified cut sets. Finally, an uncertainty analysis was performed for the plant model with the revised data, using IRRAS with Latin Hypercube Sampling and 10,000 samples (Russell and McKay).

7.2 Contribution of Manual Switchover to CDF

This section presents the results of the PRA for the case study of a representative PWR with manual switchover of ECCS to recirculation. These results include the most frequent cut sets involving switchover failure and the important basic events in the switchover failure model.

The contribution of manual switchover to CDF was determined as described above. Failures of the RHR pumps to stop and restart were included as switchover control failures because some potential modifications to the control system have the side effect of permitting continuous operation of the pumps. RWST level indication errors were also included.

Table 7.1 shows the dominant core damage sequences involving failure of recirculation, with their frequencies. Table 7.2 lists the mean frequencies for the most frequent cut sets that contain switchover control failures. The top four cut sets, accounting for 40% of the mean switchover control contribution, are accident sequences initiated by a very small LOCA (S3), followed by operator's inability to control containment sprays (OC). Some cut sets in this list are initiated by a small LOCA (S2), a medium LOCA (S1), or a large LOCA (AH1).

In the first, third, and fourth most frequent cut sets, the failure of recirculation results from coupled operator errors, one for each train, that have been modeled with complete dependence. The dominant scenario for such coupled failures is operator omission of a line in the EOP that refers to both

Table 7.1 Frequencies of Dominant Core Damage Sequences Involving ECCS Recirculation Failure at Representative PWR with Manual Switchover

Sequence Frequency (per reactor-yr)	Nomenclature	Description
2.3×10^{-5}	S3-OC-H3	Very Small LOCA -Sprays stay on - LPR fails
8.6×10^{-6}	S2-H3	Small LOCA - LPR fails
8.3×10^{-6}	S1-H4	Medium LOCA - LPR fails
5.9×10^{-6}	AH1	Large LOCA - LPR fails
4.0×10^{-6}	S3-OC-H2	Very Small LOCA - Sprays stay on - HPR fails
1.3×10^{-6}	S1-H2	Medium LOCA - HPR fails
1.3×10^{-6}	S2-H2	Small LOCA - HPR fails
5.0×10^{-7}	S3-W1-H3	Very Small LOCA - RHR fails - LPR fails
Total: 5.3×10^{-5} per reactor-yr		

Table 7.2 Most Frequent Cut Sets for Representative Manual Switchover Control Failure

Cut Set Frequency (per reactor-yr)	Cumulative Switchover Control Contribution Fraction	Initiator	Cut Set
$6.6x10^{-6}$	0.15	S3	OC LP-2122RHR-CC
$4.4x10^{-6}$	0.24	S3	OC L3-RWSTL-OP2
$4.0x10^{-6}$	0.33	S3	OC LP-2122SJ44-CC
$3.1x10^{-6}$	0.40	S3	OC HPR-HE-FO-SIMN2
$3.1x10^{-6}$	0.47	AH1	L3-RWSTL-OP1
$2.7x10^{-6}$	0.53	S2	L3-RWSTL-OP
$2.7x10^{-6}$	0.59	S1	L3-RWSTL-OP
$2.2x10^{-6}$	0.63	S2	LP-2122RHR-CC
$2.2x10^{-6}$	0.68	S1	LP-2122RHR-CC
$1.5x10^{-6}$	0.72	S3	OC LP-SUMPL-OP
$1.5x10^{-6}$	0.75	S3	OC LP-RWSTS-CC
$1.4x10^{-6}$	0.78	S3	OC LP-2122RHR-ST
$1.3x10^{-6}$	0.81	S2	LP-2122SJ44-CC
$1.3x10^{-6}$	0.84	S1	LP-2122SJ44-CC
$1.1x10^{-6}$	0.86	AH1	LP-2122RHR-CC
$1.0x10^{-6}$	0.88	S2	HPR-HE-FO-SIMIN
$1.0x10^{-6}$	0.91	S1	HPR-HE-FO-SIMIN
$0.7x10^{-6}$	0.92	AH1	LP-2122SJ44-CC
$0.5x10^{-6}$	0.93	S2	LP-SUMPL-OP
$0.5x10^{-6}$	0.94	S2	LP-RWSTS-CC
$0.5x10^{-6}$	0.95	S1	LP-SUMPL-OP
$0.5x10^{-6}$	0.96	S1	LP-RWSTS-CC
$0.4x10^{-6}$	0.97	S2	LP-2122RHR-ST
$0.4x10^{-6}$	0.98	S1	LP-2122RHR-ST
$0.3x10^{-6}$	0.99	AH1	LP-SUMPL-OP
$0.3x10^{-6}$	1.00	AH1	LP-RWSTS-CC
$0.2x10^{-6}$	1.00	AH1	LP-2122RHR-ST

trains. The first cut set results from failure to restart the RHR pumps, the third from failure to open the sump valves, and the fourth from failure to close the SI miniflow valves. In four of the top seven cut sets, amounting to 28% of the contribution to CDF, the operator fails to enter the correct EOP for switchover. Other switchover failures in the top cut sets are failure to recognize that sump level is adequate for switchover, miscalibration of RWST level sensors, and common cause failure of the RHR pumps to restart after switchover.

Table 7.3 lists the switchover basic events that offer the greatest potential for risk reduction. The value shown for each event is how much the CDF would be reduced if that event had zero probability. For this list, events representing the same failure, but in different sequences, have been combined. The top four items on this list correspond to the top four cut sets in the dominant LOCA sequence, in slightly different order.

Some results for the representative plant with manual switchover are listed below:

Table 7.3 Top Manual Switchover Control Failure Events for Contribution to CDF

Contribution to CDF (per reactor-yr)	Nomenclature	Description
$1.3x10^{-5}$	L3-RWSTL-OP or L3-RWSTL-OP1 or L3-RWSTL-OP2	Operator fails to enter EOP LOCA-3
$1.2x10^{-5}$	LP-2122RHR-CC	Operator fails to restart 21 & 22RHR pumps (CC)
$7.3x10^{-6}$	LP-2122SJ44-CC	Operator fails to open 21SJ44 & 22SJ44 (CC)
$5.1x10^{-6}$	HPR-HE-FO-SIMIN or HPR-HE-FO-SIMN1 or HPR-HE-FO-SIMN2	Operator fails to close 2SJ67, 2SJ68, and 2SJ67X (CC)
$2.8x10^{-6}$	LP-SUMPL-OP	Operator fails to respond to sump level >68%
$2.8x10^{-6}$	LP-RWSTS-CC	Miscalibration of RWST level sensors
$2.5x10^{-6}$	LP-2122RHR-ST	CC failure of RHR pumps to restart

Contributions to CDF (per reactor-yr) for representative plant with manual switchover

	5th	Mean	95th
all internal events	$1.7x10^{-5}$	$7.9x10^{-5}$	$2.2x10^{-4}$
switchover control failures	$4.2x10^{-6}$	$4.6x10^{-5}$	$1.6x10^{-4}$
coupled human errors	$2.6x10^{-6}$	$2.5x10^{-5}$	$8.2x10^{-5}$

7.3 Contribution of Semiautomatic Switchover to CDF

This section presents the results of the PRA for the case study of a representative PWR with semiautomatic ECCS to recirculation. These results include the most frequent cut sets involving switchover failure and the important basic events in the switchover failure model.

Table 7.4 shows the dominant core damage sequences involving ECCS recirculation failure, with their frequencies. Table 7.5 lists the most frequent cut sets that contain semiautomatic switchover control failures. The top three cut sets, accounting for 37% of the switchover control contribution, are accident sequences initiated by a very small LOCA (S3), followed by operator's inability to control containment sprays (OC). Some cut sets in this list are initiated by a small LOCA (S2), a medium LOCA (S1), or a large LOCA (AH1).

In the most frequent cut set, the operator fails to enter the correct EOP for switchover. In the second and third cut sets, the failure of recirculation results from an operator error on both trains, with complete dependence. The second cut set results from failure to arm the sump valves and the third from failure to close the SI miniflow valves. Other switchover failures in the top cut sets are failure to recognize that sump level is adequate for switchover, miscalibration of RWST level sensors, and common cause failure of the logic boards.

Table 7.6 lists the switchover basic events that offer the greatest potential for risk reduction. The value shown for each event is how much the CDF would be reduced if that event had zero probability. For this list, events representing the same failure, but in different sequences, have been combined. The top three items on this list correspond to the top three cut sets in the dominant LOCA sequence.

The results for the representative plant with semiautomatic switchover are listed below:

Table 7.4 Frequencies of Dominant Core Damage Sequences Involving ECCS Recirculation Failure at Representative PWR with Semiautomatic Switchover

Sequence Frequency (per reactor-yr)	Nomenclature	Description
1.4×10^{-5}	S3-OC-H3	Very Small LOCA -Sprays stay on - LPR fails
5.5×10^{-6}	S2-H3	Small LOCA - LPR fails
5.3×10^{-6}	S1-H4	Medium LOCA - LPR fails
4.0×10^{-6}	S3-OC-H2	Very Small LOCA - Sprays stay on - HPR fails
3.6×10^{-6}	AH1	Large LOCA - LPR fails
1.3×10^{-6}	S1-H2	Medium LOCA - HPR fails
1.3×10^{-6}	S2-H2	Small LOCA - HPR fails
5.0×10^{-7}	S3-W1-H3	Very Small LOCA - RHR fails - LPR fails

Total: 3.6×10^{-5} per reactor-yr

Table 7.5 Most Frequent Cut Sets for Representative Semiautomatic Switchover Control Failure

Cut Set Frequency (per reactor-yr)	Cumulative Switchover Control Contribution Fraction	Initiator	Cut Set
4.4×10^{-6}	0.14	S3	OC L3-RWSTL-OP2
3.6×10^{-6}	0.26	S3	OC LP-2122SJ44-CC
3.1×10^{-6}	0.37	S3	OC HPR-HE-FO-SIMN2
3.1×10^{-6}	0.47	AH1	L3-RWSTL-OP1
2.7×10^{-6}	0.56	S2	L3-RWSTL-OP
2.7×10^{-6}	0.64	S1	L3-RWSTL-OP
1.6×10^{-6}	0.70	S3	OC LP-SUMPL-OP
1.6×10^{-6}	0.75	S3	OC LP-RWSTS-CC
1.2×10^{-6}	0.79	S2	LP-2122SJ44-CC
1.2×10^{-6}	0.83	S1	LP-2122SJ44-CC
1.0×10^{-6}	0.86	S2	HPR-HE-FO-SIMIN
1.0×10^{-6}	0.89	S1	HPR-HE-FO-SIMIN
0.6×10^{-6}	0.91	AH1	LP-2122SJ44-CC
0.5×10^{-6}	0.93	S2	LP-SUMPL-OP
0.5×10^{-6}	0.95	S2	LP-RWSTS-CC
0.5×10^{-6}	0.96	S1	LP-SUMPL-OP
0.5×10^{-6}	0.98	S1	LP-RWSTS-CC
0.2×10^{-6}	0.99	AH1	LP-SUMPL-OP
0.2×10^{-6}	0.99	AH1	LP-RWSTS-CC
0.2×10^{-6}	1.00	S3	OC LP-LOGIC-CC

Table 7.6 Top Semiautomatic Switchover Control Failure Events for Contribution to CDF

Contribution to CDF (per reactor-yr)	Nomenclature	Description
1.3×10^{-5}	L3-RWSTL-OP or L3-RWSTL-OP1 or L3-RWSTL-OP2	Operator fails to enter EOP LOCA-3
6.6×10^{-6}	LP-2122SJ44-CC	Operator fails to arm 21SJ44 & 22SJS44 (CC)
5.1×10^{-6}	HPR-HE-FO-SIMIN or HPR-HE-FO-SIMN1 or HPR-HE-FO-SIMN2	Operator fails to close 2SJ67, 2SJ68, and 2SJ67X (CC)
2.8×10^{-6}	LP-SUMPL-OP	Operator fails to respond to sump level >68%
2.8×10^{-6}	LP-RWSTS-CC	Miscalibration of RWST level sensors
3.0×10^{-7}	LP-LOGIC-CC	Train A & B logic boards fail (CC)

Contributions to CDF (per reactor-yr) for representative plant with semiautomatic switchover

	5th	Mean	95th
all internal events	1.5×10^{-5}	6.3×10^{-5}	1.7×10^{-4}
switchover control failures	3.3×10^{-6}	3.0×10^{-5}	9.6×10^{-5}

7.4 CDF Difference Between Manual and Semiautomatic Switchover

This section discusses the calculation of the uncertainty distribution for the difference in CDF between the representative manual system and the representative semiautomatic system. The first step was calculation of the uncertainty distribution for the CDF contribution from all failure modes that are present in the manual system but are not in the semiautomatic system. In the second step, the distribution was found for the CDF contribution from failure modes unique to the semiautomatic system.

The results of these two calculations were:

Contributions to CDF (per reactor-yr) from failures unique to one type of switchover

	5th	Mean	95th
manual-only failure modes	2.6×10^{-6}	2.4×10^{-5}	7.8×10^{-5}
semiautomatic-only modes	5.8×10^{-7}	6.7×10^{-6}	2.3×10^{-5}

If the representative manual system were replaced by the representative semiautomatic system, the CDF would be reduced by eliminating the manual-only modes, but increased by the introduction of any new failure modes in the semiautomatic system. The new failure modes would be not only those in the new control logic, but also any that might be introduced by the revision of the EOP.

The reduction in CDF is given by:

$$\Delta(\text{CDF}) = \text{CDF}_{\text{Manual}} - \text{CDF}_{\text{Semiautomatic}}$$

where Δ(CDF) is the CDF difference. Note that a negative reduction represents an increase in accident frequency from the base to the adjusted case, i.e., an increase resulting from the proposed action.

The uncertainty distribution for the CDF difference was obtained using approximations to the two calculated uncertainty distributions. Both calculated distributions were approximated by log-normal distributions, with means equal to the calculated means

and error factors of 6 about the corresponding medians. These distributions matched the percentiles reported above to within 18%.

With these approximations and taking advantage of the stochastic independence of the two uncertainty distributions, the distribution for the CDF difference was evaluated numerically. The resulting distribution for the CDF difference has the following properties:

CDF change (per reactor-yr) if representative manual system were replaced by representative semiautomatic system

5th	Mean	95th
-1×10^{-5}	1.7×10^{-5}	7×10^{-5}

This distribution crosses zero at the 22nd percentile; the probability that the change will result in a CDF increase is about 22%.

8.0 Population Dose per Core Damage Event

This section estimates the risk to public health given that a failure of ECCS switchover has resulted in core damage. In accordance with the proposed NRC regulatory analysis guidelines, changes in public health and safety from radiation and offsite property impacts were considered over a 50-mile distance from the plant site.

The representative plant has a large, dry containment, as do 36 of the 39 PWRs that are listed in Appendix C as having manual switchover. Estimates for other containments were also obtained.

The NUREG-1150 back-end analysis for Sequoyah (Gregory and Murfin) notes that the arrest of core damage before vessel breach plays an important part in reducing the risk due to LOCAs. Furthermore, depressurization of the RCS before the vessel fails is important in reducing the loads placed upon the containment at vessel breach and in arresting core damage before vessel breach. These observations are consistent with the conditional probabilities of early containment failure reported for three PWRs, as follows (NRC, NUREG-1150):

Conditional probabilities of early containment failure for LOCAs and for all internal events

Plant	Containment	LOCA	all
Zion	Large Dry	0.01	0.01
Sequoyah	Ice Condenser	0.04	0.07
Surry	Sub-Atmospheric	0.006	0.008

The conditional probabilities for all internal events are not much larger than the those for LOCAs, especially in the case of the large, dry containment. For purposes of cost-benefit estimates, the 50-mile doses from all internal events were used to estimate the LOCA risk.

For each containment type, the uncertainty distribution for 50-mile dose was estimated by approximating two other uncertainty distributions and combining the results. One of these distributions was the CDF for internal events. The distributions reported in NUREG-1150 are:

CDF (per reactor-yr) per NUREG-1150

	5th	Mean	95th
Zion: Dry	1.1×10^{-4}	3.4×10^{-4}	8.4×10^{-4}
Sequoyah: Ice	1.2×10^{-5}	5.7×10^{-5}	1.8×10^{-4}
Surry: Sub-Atmospheric	6.8×10^{-6}	4.0×10^{-5}	1.3×10^{-4}

The other distributions that were approximated were for the public dose within 50 miles. The NUREG-1150 results were:

50-mile dose (person-rem per reactor-yr) per NUREG-1150

	5th	Mean	95th
Zion: Dry	3.5	50	170
Sequoyah: Ice	0.5	12	50
Surry: Sub-Atmospheric	0.25	5.5	30

Each of these six uncertainty distributions was approximated by a log-normal distribution. The approximations given below provide an exact match for the mean and are within 20% of the 5th and 95th percentiles in all but one case:

CDF (per reactor-yr) as approximated

	Mean	Error factor
Zion: Large Dry	3.4×10^{-4}	3
Sequoyah: Ice Condenser	5.7×10^{-5}	4
Surry: Sub-Atmospheric	4.0×10^{-5}	4

50-mile dose (person-rem per reactor-yr) as approximated

	Mean	Error factor
Zion: Large Dry	50	7
Sequoyah: Ice Condenser	12	10
Surry: Sub-Atmospheric	5	10

For each containment type, there is a unique log-normal distribution for 50-mile dose per event that is consistent with the approximate distributions. These derived functions are described below:

50-mile dose per event (person-rem)

	Mean	Error factor
Zion: Large Dry	1.5×10^{5}	4
Sequoyah: Ice Condenser	2×10^{5}	7
Surry: Sub-Atmospheric	1×10^{5}	7

9.0 Selection of Potential Alternatives for Cost/Benefit Analysis

9.1 Safety Goal Evaluations

To provide direction in deciding whether a potential generic safety enhancement backfit meets the substantial additional protection standard of the backfit rule (10 CFR 50.109), draft NRC guidelines call for a safety goal evaluation (NRC, SECY-93-167). The results of Sections 7 and 8 provide sufficient information for a safety goal evaluation of each of the potential alternatives that were listed in Section 2.6. In particular, because the estimated conditional containment failure probability is no more than 0.1, the draft guidelines suggest that a potential decrease in CDF of at least $1x10^{-5}$ per reactor-yr would be needed to justify further analysis. This section estimates the mean change in CDF that would result from each potential alternative.

9.1.1 Single-Failure Criterion for Manual Valve and Pump Operations

This alternative requires that EOPs be modified as necessary to assure that switchover can be accomplished assuming one operator error in valve or pump operations. It applies to both manual and semiautomatic systems.

The CDF reduction available through this alternative was estimated to be the contribution to CDF from the coupled human errors that would either become uncoupled or would otherwise cease to be single-point failures of switchover. For the representative manual system, the mean CDF contribution from such failure events was $2.5x10^{-5}$ per reactor-yr. This potential alternative is analyzed in Section 11.

9.1.2 Requiring Continuous Flow

If a manual system were modified to eliminate stopping and restarting the pumps, it would eliminate all potential failures of the pumps to stop and restart, as well as all potential operator errors in those steps. The mean contribution of these failure events to the CDF for the representative manual system was found to be $1.5x10^{-5}$ per reactor-yr.

More than two-thirds of this contribution is from coupled operator errors which could be eliminated with less expense by adopting the previously discussed alternative. The potential additional reduction in CDF, $2.5x10^{-6}$ per reactor-yr, is too small to justify further analysis. Consequently this potential alternative was not analyzed further.

9.1.3 Requiring Semiautomatic Switchover

The potential CDF reduction from conversion of a manual system to a semiautomatic system with manual actuation can be estimated from the results reported in Section 7.4 for the representative systems. The mean value was found to be $1.7x10^{-5}$ per reactor-yr, which is sufficient to permit further analysis. The cost-benefit analysis for this potential alternative appears in Section 10.

9.1.4 Requiring Semiautomatic Switchover With Automatic Actuation

This option is the same as the one just discussed except that there is a further potential CDF reduction, at most $1.6x10^{-5}$ per reactor-yr, from eliminating failures to diagnose the need for switchover and to initiate switchover at the correct time. The savings are reduced by the potential failure by the automatic system. However, the dominant mode of failure of automatic actuation would be common cause failure of the redundant batteries, which is already included.

This option is not analyzed separately. Instead, it is discussed at the end of Section 10.

9.1.5 Requiring Complete Automation of ECCS Switchover

As discussed in Section 4, conversion of a manual system to fully automatic may require much more extensive modifications than a change to semiautomatic.
The Salem 2 licensee found that some potential changes would result in ECCS vulnerability to a single component failure. Avoiding this problem might not be possible without a complete redesign and replacement of the ECCS system.

The potential benefit may be estimated from Table 7.6. The maximum CDF reduction is that which would occur if all dominant failures were removed

except logic failures and miscalibration of the RWST level sensors. This would reduce the mean CDF contribution of switchover control to $3x10^{-6}$ per reactor-yr. That would constitute a reduction of $4.3x10^{-5}$ per reactor-yr from the mean for the representative manual system that is reported in Section 7.2.

9.2 General Assumptions and Bases for Cost-Benefit Studies

Sections 10 and 11 present cost-benefit analyses for implementation of certain backfit requirements for control of switchover of ECCS to recirculation. The estimates of benefits to public health made use of the results reported in Sections 7 and 8.

The cost-benefit analyses assumed that a potential improvement to ECCS switchover to recirculation would be a backfit that applied to the 36 PWRs that are identified in Appendix C as having manual switchover systems. Their average license expiration date being the end of 2013, the remaining facility life was assumed to be 19 years without license renewal and 39 years with license renewal.

Costs to both the Licensee and the NRC were considered, with uncertainty. These include uncertainties in the costs of particular elements as well as differences in the modifications necessary from one plant to another. The estimates developed also account for cost impacts related to plant life extension and license renewal.

The following assumptions and bases were used in developing the cost-benefit estimates:

- All costs are in 1994 dollars.
- The public exposures consequent to failures to complete switchover were based on the fit to 50-mile dose per Zion LOCA that was reported at the end of Section 8. This estimate is 1.5 $x10^5$ person-rem, with an error factor of 4.
- The value of $1,000 per person-rem, without uncertainty, was used as a conversion factor for all offsite consequences of severe accidents, including both public health and offsite property effects. Because this was taken as a point value, the probability that the net cost will be less than $1,000 per person-rem is the same as the probability that the net of all values and impacts will be positive.
- Occupational exposure per core damage event was calculated using fits to the values suggested in the Regulatory Analysis Handbook. The fits were 1000 person-rem (EF=10) of short-term exposure and 20,000 person-rem (EF=1.6) spread over 10 years.
- As with public health, a value of $1,000 per person-rem (no uncertainty) was used for monetary conversion of occupational exposure.
- Base labor hours and equipment costs associated with the candidate plant modifications were derived primarily from NRC's generic cost estimation methodology (NRC, NUREG/CR-4627 and -5160). Where generic information was not available, equipment costs and labor hour estimates were based on vendor quotes and/or engineering judgement. NRC's generic cost estimation methodology utilizes new construction cost and labor data for a nuclear plant environment. Labor estimates from this source had to be adjusted to reflect operating nuclear plant conditions. Factors such as radiation, congestion, and access typically contribute to reduce labor productivity at operating plants. In addition, the costs were escalated to reflect 1994 dollars. Adjustment to the base labor estimates were made according to the NRC guidelines (NRC, NUREG/CR-4627).
- Implementation activities are assumed to be incurred immediately. That is, they are presented on an "overnight" cost basis and are not discounted.
- Recurring costs are assumed to be incurred annually for the remaining life of the plant. Remaining plant life is assumed to be 19 years without license renewal and 39 years with license renewal. Costs incurred in future years are discounted (present-valued) using a discount rate of 7%.
- Averted onsite property impacts were taken to include both averted cleanup and decontamination costs and averted replacement power costs and were discounted

at 7%. Because recovery of ECCS is likely to limit the degree of damage, estimates for the mean cleanup and decontamination cost per core damage event were based on "Scenario 1," in which some fuel cladding ruptures, no fuel melts, the containment building is moderately contaminated, and there is minimal physical damage. An error factor of two was used to reflect the uncertainty in the degree of damage.

- This study used estimates of replacement power costs developed by Argonne National Laboratory for NRC regulatory analysis, with an error factor of 1.2 and a discount rate of 7%. Replacement power costs were applied for the remaining reactor lifetime (19 or 39 years).

- Best estimates were assumed to be means of log-normal distributions unless otherwise stated. Labor rates were assumed to have an error factor of 1.25.

10.0 Net Value of Changeover to Semiautomatic ECCS Switchover to Recirculation

10.1 Major Cost Elements

The major cost elements associated with implementation of a semiautomatic ECCS switchover system are as follows:

Costs to Licensee:

Physical Modifications
- Addition of check valves
- Addition of logic controller and associated control circuits to affected motor operated valves (MOVs)
- Modifications to plant simulator

Analytical/Procedural Costs: Engineering Analysis
- FMEA or update to plant PRA
- Cost/Benefit Analysis
- Transient Analysis

Procedural Changes
- Changes to operator training courses
- Revised operator training
- Revisions to plant operating procedures
- Technical specification changes

Operations and Maintenance (O&M) Costs

Periodic inspection, surveillance, test and maintenance (ISTM) of additional check valves and MOVs with modified control functions

Costs to the NRC:

- Review of Technical Specification Changes
- Inspection of Physical Modifications

The foregoing listing includes both one-time and recurring costs. For the physical modifications cited above, several types of costs are applicable to the current cost assessment. In addition, any additional occupational radiation exposure associated with the switchover changes must be accounted for. Thus, the physical modifications impact assessment should include the following:

- Cost of materials and equipment
- Installation costs
- Engineering and quality assurance costs
- Health physics support costs
- Occupational radiation exposure associated with hardware installation or modification, and with subsequent ISTM of the affected components or hardware

10.2 Cost Assumptions and Bases

The following assumptions and bases were used in developing the cost estimates for implementing semiautomatic ECCS switchover to recirculation:

- The costs are based largely on the design described in Section 4.

- The estimates apply to a single plant. For multiple unit sites, the assumption is that there are no shared systems relative to the physical modifications or procedural changes contemplated. However, simulators may serve more than one plant.

- Plant modifications, if required, can be made during plant operation or during scheduled outages. These modifications will not require any incremental plant down time, and, therefore, do not involve any replacement energy costs.

- Physical modifications made in a radiation environment, such as the addition of check valves to the RHR suction lines, require health physics (HP) support services. HP-related services are costed at the rate of $10,900 per person-rem incurred. The general area radiation field in the vicinity of the RHR pump suction lines was taken to have a best estimate (mean) of 15 millirem per hour, with uncertainty represented by a log-normal distribution with an error factor of 1.3.

10.3 Overall Cost and Benefit Estimates

10.3.1 Benefits

The benefits of the changeover from manual to semiautomatic are based on the difference between the corresponding log-normal distributions with means of 2.4×10^{-5} and 6.7×10^{-6} per reactor-yr, for the

manual-only and semiautomatic-only failure modes contributions to CDF, respectively; the error factors in both cases are set equal to 6.

10.3.2 Licensee Costs

10.3.2.1 Physical Modification Costs

Addition of Check Valves

The Representative Plant evaluation suggested that two check valves should be installed in the suction line to each RHR pump, one in the suction line from the containment sump and one in the suction line from the RWST. On examination of the details from a similar plant (Zion Units 1 and 2, 1040 MWe each) indicated that the piping from the RWST is 12 inches in diameter, and the suction piping from the containment sump is 18 inches in diameter. These diameters were taken to be representative of the sizes applicable to a large number of plants, and were used for the "best" estimates. The two 12-inch check valves are estimated to cost about $5,500 each, and the 18-inch valves almost $15,000 each. These costs are based on the use of carbon steel valves. "Greenfield" or new construction installation was estimated to require about 130 hours of labor. A labor allowance was also included to account for removal of a section of pipe in order to place the check valves in the appropriate suction line locations. Engineering and quality assurance costs are assumed to be 25% of the direct labor, equipment, and hardware costs.

Some plants (such as the Representative Plant) may get by with installing only two check valves rather than the four included in the best estimate. A more complex arrangement might entail installation of six valves. To include this uncertainty, labor hours and equipment costs were assigned an error factor of 2.

Addition of Logic Controller and Control Line to Affected MOVs

The logic controller needed for the conversion of the ECCS to semiautomatic switchover can be fairly simple, and a basic unit is estimated to cost about $3,500. Because of its important safety function, however, the best estimate case assumes that the controller must be qualified to class 1E requirements, with an attendant increase in controller costs to $35,000. Also, redundant control circuits must be run between the logic controller and each of the affected MOVs. The Representative Plant evaluations indicate that four MOVs per train would be impacted by the modification to semiautomatic switchover. Each of the eight circuits is estimated to cost about $2,000 in hardware and about 13 labor hours for (Greenfield) installation. This labor estimate is adjusted to account for reduced labor productivity in an operating plant environment and in a radiation area.

The best estimate cost assumes that a Class 1E controller is installed, but that only single control circuits are run to each affected MOV (existing wiring is assumed to be used for one of the redundant circuits to each MOV). The costs will be higher if two circuits must be run to each MOV. On the other hand, the controller may not need to be qualified to Class 1E standards, and that existing control circuits may largely be used. To reflect these uncertainties, error factors of 2 were assigned to labor hours and equipment costs.

Occupational radiation exposure associated with this installation activity is estimated to be about one person-rem per plant.

Simulator Modifications

The change from manual to semiautomatic switchover of ECCS to recirculation requires that the plant simulator be modified as well. The control panels must be changed, as must the simulator logic (programming). The associated costs will depend on the complexity and flexibility of the simulator, as well as whether or not the simulator applies to a single unit or multiple units.

The best estimate assumes that the simulator modifications can be made with a reasonably modest effort that includes design engineering, re-programming/logic changes, modifications to the simulator panels and displays, and checkout and verification of the changes. Because some simulators may be more difficult to modify and some simulators are used for multiple plants, with a reduced cost on a per-plant basis, an error factor of 2 was applied.

10.3.2.2 Analytical/Procedural Costs

Engineering Analysis

Three types of engineering evaluations are envisioned as necessary in order to convert from manual to semiautomatic switchover of ECCS to recirculation. The first is a failure mode and effects analysis (FMEA) and/or updating of the plant Individual Plant Examination (IPE) or plant probabilistic safety assessment (PSA). This analysis is needed to assess, on a plant-specific basis, the safety implications of the change to semiautomatic switchover. A minimal effort might produce a detailed FMEA to identify vulnerabilities and strengths of alternative designs. It involves gathering data, performing the FMEA, and having the work reviewed. This work is estimated to require about one person-month to accomplish. The best estimate assumes that the plant PSA is updated and used to evaluate alternative configurations. It would involve the development of new fault trees for the portions of the ECCS impacted by the proposed changes, and generating and quantifying new cut-sets. This effort is judged to require about four person-months of effort at a fully loaded rate of $74 per hr. However, the evaluations may be more extensive and the modifications of interest may be more complex than is the case for the best estimate.

The cost/benefit analysis develops cost estimates for proposed alternatives and compares them against the likely benefits. This effort assists in selecting the preferred or best alternative among the design choices. The effort was estimated to require three person-months.

An additional engineering analysis deemed necessary is the transient analyses to model the dynamics of the ECCS switchover in the semiautomatic mode. This analysis would assess the adequacy of the sump NPSH during the switchover. Transient effects would be evaluated to help establish the best sizing and configuration of components to be added, their dynamic characteristics, and the timing and time windows available or preferred for the valve closings and openings, etc. This analysis would entail development or modification of analytical models, exercising the models, evaluating and reviewing the results, and translating these into preliminary engineering specifications for the chosen modifications. This effort is estimated to require two (minimum) to five (maximum) person-months to accomplish, with a best estimate of three.

An error factor of 2 was used to cover the various uncertainties in the required analytical effort

One-Time Costs Related to Operator Training and Technical Specification Change

Operators must be trained in the semiautomatic switchover of ECCS to recirculation. One time costs will be incurred in revising operator training course materials. In addition, the operating procedures must be revised. The course revision costs are estimated using a cost of $146/page of revised course materials. Based on materials available from the Representative Plant, about 15 pages are assumed to be involved, with an error factor of 2. These material explain the philosophy and approach taken for semiautomatic switchover, the specific components involved, the operator's role, etc. The $146/page charge is based on NRC's generic cost estimation methodology (NRC, NUREG/CR-4627).

The operating procedures must also be rewritten to guide operators in the steps they must follow to successfully accomplish ECCS switchover to recirculation. The effort required is judged to be a "complex" change per NRC's generic cost estimation methodology, and has an associated cost of about $5,300 per plant, with an error factor of 1.3.

The plant technical specifications must also be changed to reflect the ECCS switchover changes. This is judged to be a routine change for the best estimate. The generic cost estimation methodology gives a cost of about $24,000 for such an effort. An error factor of 2 was used to cover the uncertainty in the complexity.

10.3.2.3 Licensee Recurring Costs

Two types of recurring costs are associated with ECCS switchover changes. The first is the additional ISTM activities associated with the additional check valves installed in the ECCS and with the logic controller and MOVs involved. The second is the change in operator training involved in making ECCS switchover to recirculation semiautomatic.

The ISTM of the newly installed check valves will entail periodic checks and refurbishment to assure that they are functioning properly. This effort is estimated to require about 16 labor-hours per valve per year. The incremental ISTM for the logic controller and MOVs involved in ECCS switchover to recirculation is estimated to require the equivalent of about 4 labor-hours per valve per year. Note that the MOVs involved are existing valves that already receive periodic testing, inspection, and maintenance. The allowance of four hours per valve per year is the incremental effort over and above the existing efforts, and accounts for the logic controller functional testing as well. The total annual impact is estimated to be $3,500 and one person-rem, plus associated health physics costs.

These incremental ISTM activities are assumed to be needed for the duration of the plant life. Without license renewal the remaining plant life is assumed to be 19 years. With license renewal, the remaining life is assumed to be 39 years.

Operator training with semiautomatic switchover of ECCS to recirculation is actually expected to be simplified somewhat compared to that needed with manual switchover. At the Representative Plant all reactor operators receive eight weeks of training annually. There are three operators per shift, and about five shifts, for a total of about 15 operators. With manual switchover of ECCS, the operators had to be trained to perform 30 steps in the switchover procedure. With semiautomatic switchover, the number of steps was reduced from 30 to 26. This experience can be used to estimate possible reductions in operator training expenses.

Training relative to ECCS switchover to recirculation is estimated to occupy from 2 to 5 days of the 8 weeks each operator receives annually. The reduction in the number of steps the operators must go through with semiautomatic switchover is about 15% of the total switchover training time, or about 2 to 6 hours of the related training time per operator. The time savings is assumed to be divided equally between classroom training time and simulator time. Using NRC generic cost estimation methodology, this translates into annual cost savings of about $2,500, offsetting some of the direct labor costs of ISTM. To cover the uncertainties, the net change in annual direct labor cost was assumed to have a uniform distribution from -$1,500 to +$3,500. The annual exposure was assigned an error factor of 2.

10.3.3 NRC Costs

The NRC is expected to incur one-time costs for two activities related to changes from manual to semiautomatic switchover of ECCS to recirculation. The first is the review of the licensees technical specification change. The costs of this review are taken from NRC's generic cost estimation methodology for a routine technical specification change, with an error factor of 2 to cover the uncertainty in the complexity.

The second cost anticipated for the NRC is that associated with performing an inspection of the physical and procedural modifications made by the licensee. The effort required for these inspections is estimated to be about three person-weeks for the best estimate. At a fully burdened labor rate of $52/hr, this results in a cost of about $6,300 for the best estimate. An error factor of 1.25 covers the anticipated variation in NRC inspection efforts.

Both the technical specification review effort and the inspection effort are one-time costs for the NRC. Recurring costs are not judged to be applicable for the NRC's efforts.

10.4 Estimated Net Value

Table 10.1 presents the overall cost and benefit estimates for implementation of semiautomatic ECCS switchover to recirculation, as calculated by the FORECAST computer code (Lopez and Sciacca); costs are negative in Table 10.1. For each attribute of the implementation, low, best, and high estimates are provided. These are the 5th percentile, the mean, and the 95th percentile of the uncertainty distribution.

The estimated mean result with license renewal is a negative net value, a net impact of about $4 million. The reported mean and percentiles for net value may be fit to a uniform distribution with a minimum of -$29.5 million and a maximum of $21.5 million, suggesting that there is approximately a 40% probability that the net cost is less than $1000 per person-rem saved

Without license renewal, the mean net value is about -$9 million. Fitting the results to a uniform distribution results in a probability of only about

Table 10.1 Estimated Attributes and Net Value of Changeover of All Manual Systems to Representative Semiautomatic System

Attribute Values (Million of Dollars)		Without License Renewal	With License Renewal
Public Health (Accident)	High	4	5
	Best	0.9	1
	Low	-5	-0.6
Occupational Health (Accident)	High	0.3	0.3
	Best	0.09	0.1
	Low	-0.06	-0.07
Occupational Health (Routine)	High	-0.05	-0.06
	Best	-0.4	-0.5
	Low	-1	-2
Onsite Property	High	20	35
	Best	7	13
	Low	-5	-8
Industry Implementation	High	-8	-8
	Best	-12	-12
	Low	-16	-16
Industry Operation	High	-2	-3
	Best	-5	-6
	Low	-8	-11
NRC Implementation	High	-0.4	-0.4
	Best	-0.7	-0.7
	Low	-1	-1
Net Value (Million of Dollars)	High	5	19
	Best	-9	-4
	Low	-22	-26

20% that the net cost will be less than $1000 per person-rem.

10.5 Scoping Analyses of Variations

10.5.1 Semiautomatic With Automatic Actuation

One variation in the analyzed alternative would be to include automatic actuation of the semiautomatic system. This entails some increase in the costs but might increase the averted exposure by as much as a factor of two.

This study did not include a calculation of the uncertainty distribution for the change of CDF for this option nor for the costs of implementation. However, a scoping cost-benefit analysis was performed under the optimistic assumption that the CDF decreased by an additional 1.6×10^{-5} per reactor-yr (no uncertainty) and that there was no additional cost.

As shown in Table 10.2, including automatic actuation in a modification to semiautomatic may offer a mean net value of as much as $9 million with license renewal. Fitting these optimistic scoping results with a uniform distribution yields about an 80% probability that the net cost is less than $1000. Without license renewal the optimistic probability is about 45% and the net value is approximately -$1 million.

10.5.2 Fully Automatic

Another variation is a backfit modification that results in a fully automatic system. This has the potential for tripling the averted CDF, but the analysis quoted in Section 4 indicates that such a conversion may require a much more extensive modification to the RHR system to satisfy the single failure criterion and assure adequate NPSH.

For an optimistic scoping cost-benefit analysis, the CDF decreased by 4.3×10^{-5} per reactor-yr (no uncertainty) from the analyzed representative manual system. The modification costs and exposures were doubled, but all other costs were unchanged.

As shown in Table 10.3, this option may offer a mean net value of as much as $13 million with license renewal. Fitting these optimistic scoping results with a uniform distribution yields a greater than 95% probability that the net cost is less than $1000. Without license renewal the optimistic probability is about 50% and the net value is approximately zero.

Table 10.2 Scoping Analysis of Changeover of All Manual Switchover Systems to Semiautomatic with Automatic Actuation

Attribute Values (Million of Dollars)		Without License Renewal	With License Renewal
Public Health (Accident)	High	5	7
	Best	2	2
	Low	0.3	0.3
Occupational Health (Accident)	High	0.3	0.4
	Best	0.2	0.2
	Low	0.09	0.1
Occupational Health (Routine)	High	-0.05	-0.06
	Best	-0.4	-0.5
	Low	-1	-2
Onsite Property	High	21	37
	Best	14	25
	Low	8	14
Industry Implementation	High	-8	-8
	Best	-12	-12
	Low	-16	-16
Industry Operation	High	-2	-3
	Best	-5	-6
	Low	-8	-11
NRC Implementation	High	-0.4	-0.4
	Best	-0.7	-0.7
	Low	-1	-1
Net Value (Million of Dollars)	High	8	23
	Best	-1	9
	Low	-10	-4

Table 10.3 Scoping Analysis of Changeover of All Manual Switchover Systems to Fully Automatic

Attribute Values (Million of Dollars)		Without License Renewal	With License Renewal
Public Health (Accident)	High	7	8
	Best	2	3
	Low	0.4	0.5
Occupational Health (Accident)	High	0.4	0.5
	Best	0.2	0.3
	Low	0.1	0.2
Occupational Health (Routine)	High	-0.05	-0.06
	Best	-0.4	-0.5
	Low	-1	-2
Onsite Property	High	23	40
	Best	18	32
	Low	14	25
Industry Implementation	High	-11	-11
	Best	-15	-15
	Low	-21	-21
Industry Operation	High	-2	-3
	Best	-5	-6
	Low	-8	-11
NRC Implementation	High	-0.4	-0.4
	Best	-0.7	-0.7
	Low	-1	-1
Net Value (Million of Dollars)	High	8	24
	Best	-0.5	13
	Low	-9	2

11.0 Net Value of a Single Failure Criterion for Train Manipulations

11.1 Major Cost Elements

The single failure criterion for manual valve and pump operations could be met at the representative plant by modifying the EOPs for switchover so that one train is switched over at a time. The major cost elements associated with the establishment of the criterion are as follows:

Costs to Licensee:

Procedural Changes
- Revisions to plant operating procedures
- Changes to operator training courses

Costs to the NRC:

- Inspection of EOPs

The foregoing listing includes one-time costs. There are no changes in recurring costs.

The estimates apply to a single plant. For multiple unit sites, the assumption is that there are no shared systems relative to the procedural changes contemplated.

11.2 Overall Cost and Benefit Estimates

11.2.1 Benefits

The benefits of adopting the criterion are based on a CDF reduction of 2.5×10^{-5} per reactor-yr (EF=6), which is a fit to the contribution of coupled human errors that was reported in Section 7.2.

11.2.2 Licensee Costs

The effort required to rewrite the operating procedures was judged to be a "complex" change per NRC's generic cost estimation methodology, which has an associated cost of about $5,300 per plant, with an error factor of 1.3.

Operators must be trained in the new procedures. One time costs will be incurred in revising operator training course materials. The course revision costs are estimated using a cost of $146/page of revised course materials. Based on materials available from the Representative Plant, about 15 pages are assumed to be involved, with an error factor of 2. These materials explain the philosophy and approach taken for semiautomatic switchover, the specific components involved, the operator's role, etc. The $146/page charge is based on NRC's generic cost estimation methodology (NRC, NUREG/CR-4627).

11.2.3 NRC Costs

The NRC is expected to incur one-time costs associated with performing an inspection of the and procedural modifications made by the licensee. The effort required for these inspections is estimated to be about two person-weeks for the best estimate. At a fully burdened labor rate of $52/hr, this results in a cost of about $4,200 for the best estimate. An error factor of 1.25 covers the anticipated variation in NRC inspection efforts.

11.3 Estimated Net Value

Table 11.1 presents the overall cost and benefit estimates for backfitting to meet a single failure criterion for manual valve and pump operations; costs are negative in Table 11.1. For each attribute of the implementation, low, best, and high estimates are provided. These are the 5th percentile, the mean, and the 95th percentile of the uncertainty distribution.

The results indicate that the backfit has an expected net value of approximately $16 million dollars, assuming relicensing. Without relicensing, the net value is about $9 million. The 5th percentiles are positive; that is, there is a greater than 95% probability that the net costs will be less than $1000 per person-rem.

Table 11.1 Attributes and Net Value of a Backfit of All Manual Switchover Systems to a Single Failure Criterion for Train Manipulations

Attribute Values (Million of Dollars)		Without License Renewal	With License Renewal
Public Health (Accident)	High	5	6
	Best	0.9	1
	Low	0.006	0.007
Occupational Health (Accident)	High	0.5	0.7
	Best	0.1	0.2
	Low	0.006	0.008
Occupational Health (Routine)	High	0	0
	Best	0	0
	Low	0	0
Onsite Property	High	42	74
	Best	9	16
	Low	0.4	0.6
Industry Implementation	High	-0.2	-0.2
	Best	-0.3	-0.3
	Low	-0.4	-0.4
Industry Operation	High	0	0
	Best	0	0
	Low	0	0
NRC Implementation	High	-0.1	-0.1
	Best	-1.5	-1.5
	Low	-2	-2
Net Value (Million of Dollars)	High	42	74
	Best	9	16
	Low	0.2	0.5

12.0 Conclusions

The ECCS is a safety system that is called upon when the rate of loss of reactor coolant through a break in the system exceeds the capability of the reactor coolant makeup system. It includes a high-pressure system and a low-pressure system so that cooling can be maintained over the variety of conditions possible during a LOCA.

At first, the ECCS draws water from the Refueling Water Storage Tank. By the time that source is exhausted, the coolant lost in a PWR will have pooled on the floor of the containment building and can be recirculated from the containment sump. Successful switchover of the ECCS from the tank to the containment sump is necessary to assure long-term cooling in a PWR following a break in the reactor cooling system.

Newer PWRs have been designed such that the ECCS switchover process is automated to some degree; earlier plants have completely manual systems. Based on plant experience and previous studies, the following suggested themselves as potentially valuable backfits to the manual systems:

- Requiring that EOPs be modified as necessary to assure that switchover can be accomplished assuming one operator error in valve or pump operations (manual and semiautomatic systems),
- Requiring modification to eliminate stopping and restarting the pumps (manual systems only),
- Requiring that valve operations for low-pressure switchover be sequenced automatically once actuated (conversion to semiautomatic, applicable to manual systems only),
- Requiring that valve operations for low-pressure switchover be actuated and sequenced automatically (manual and semiautomatic systems),
- Requiring that valve operations for low-pressure and high-pressure switchover be actuated and sequenced automatically (conversion to fully automatic, applicable to manual and semiautomatic systems).

In order to evaluate these alternatives, two failure models were developed for a representative PWR, one with manual switchover of ECCS to recirculation and one with a semiautomatic system. The semiautomatic system was assumed to rely on the operators for diagnosis of the need to switchover and recognition that the time for switchover had arrived. The semiautomatic system would complete the sequencing of low-pressure switchover but leave completion of high-pressure switchover for the operators. The models were supported by a human reliability analysis of the switchover procedures that took into consideration details of the control panels and the operating procedures in the representative PWR.

The method used in this study analyzed in detail the modification from manual to semiautomatic ECCS switchover to recirculation at the representative plant, but incorporated these models in the NUREG-1150 PRA models for the Sequoyah plant to calculate the corresponding CDFs; in addition, the public exposures consequent to failures to complete switchover were based on the 50-mile dose estimate for the Zion plant. It is recognized that this combination of available models introduces additional uncertainties, but it was beyond the scope of this study to develop the specific PRA models for the representative plant.

The failure models were evaluated with a treatment of uncertainty. The mean contributions to core damage frequency were found to be 2.4×10^{-5} per reactor-yr for the manual-only failure modes and 6.7×10^{-6} per reactor-yr for the semiautomatic-only failure modes. The mean reduction in core damage frequency resulting from conversion to semiautomatic was found to be 1.7×10^{-5} per reactor-yr.

Over 90% of the PWRs with manual switchover have a large, dry containment. An NRC-sponsored PRA for a PWR with such a containment found that the conditional probability of early containment failure following a LOCA is 0.01. Further analysis of the reported results found that the mean 50-mile dose given a LOCA is 1.5×10^5 person-rem. Results for other containment types were in the range of 1×10^5 to 2×10^5 person-rem.

Because of the relatively low conditional probability of containment failure, a backfit alternative would have to offer a potential decrease in core damage

frequency of at least $1x10^{-5}$ per reactor-yr to justify further analysis. On this basis, a backfit to just achieve continuous flow was eliminated in comparison with the backfit to a single failure criterion for manual valve and pump operations.

A detailed cost-benefit analysis for conversion from manual to semiautomatic found that the net cost of the modification would be more likely than not to exceed $1000 person-rem. Scoping analyses of additional automation and optimistic assumptions with respect to the reduction in CDF and costs associated to the modifications, indicate that the probability of meeting the $1000-per-person-rem criterion would be about 50% without license renewal or over 95% with license renewal.

The remaining alternative, a backfit to a single failure criterion for certain manual operations, was assumed to be possible with only changes in the details of the operating procedures. Because of the relatively low assumed cost, this alternative was found to offer more than a 95% probability of a positive net value.

13.0 References

Beckjord, E., NRC, Memorandum to W. Minners, "Generic Issue No. 24, 'Automatic Emergency Core Cooling Switchover to Recirculation,'" July 23, 1991.

Bertucio, R., and S. Brown, NUREG/CR-4550, Vol. 5, Rev. 1, "Analysis of Core Damage Frequency: Sequoyah, Unit 1 Internal Events," Sandia National Laboratories, April 1990.

Breeding, R., J. Helton, W. Murfin, and L. Smith, NUREG/CR-4551, Vol. 3, Rev. 1, "Evaluation of Severe Accident Risks: Surry Unit 1," Sandia National Laboratories, October 1990.

Carolina Power & Light Company, "H. B. Robinson Steam Electric Plant Unit No. 2 Individual Plant Examination Submittal," Raleigh, August 1992.

Department of Defense, MIL-HDBK-217F, "Reliability Prediction of Electronic Equipment," December 2, 1991.

Gregory, J.,W. Murfin, S. Higgins, R. Breeding, J. Helton, and A. Shiver, NUREG/CR-4551, Vol. 5, Rev. 1, "Evaluation of Severe Accident Risks: Sequoyah, Unit 1," Sandia National Laboratories, December 1990.

Hall, R. E., J. Fragola, J. Wreathall, NUREG/CR-3010, "Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation," 1982.

Heaberlin, S., J. Burnham, R. Gallucci, M. Mullen, R. Nesse, L. Nieves, J. Tawil, M. Triplett, S. Weakley, and A. Wusterbarth, NUREG/CR-3568, "A Handbook for Value-Impact Assessment," Pacific Northwest Laboratory, December 1983.

Hodges, M., NRC Memorandum to W. Lanning , "Long-Term Follow-up on Post-LOCA ECCS Recirculation Switchover (TAC 66653)," May 1, 1989.

Lopez, B., and F. W. Sciacca, "FORECAST, Regulatory Effects Cost Analysis Software Manual, Version 4.0 Beta," SEA94-706-10-A:1, Science & Engineering Associates, Inc., June 1994.

Mittl, R. L., Public Service Electric and Gas, to Director of Nuclear Reactor Regulation, ATTN: Mr. A. Schwencer, LB#3, "Proposed Conceptual Design, ECCS Automatic Switchover, No. 2 Unit, Salem Nuclear Generating Station, Docket No. 50-311," July 17, 1980.

Northeast Utilities, "Haddam Neck Plant Individual Plant Examination for Severe Accident Vulnerabilities," NRC Docket No. 50-213, B1450, Hartford, CT, June 1993.

NRC, NUREG-0800, "Standard Review Plan," Appendix 7-1, "Branch Technical Positions (ICSB)," Branch Technical Position ICSB 20, "Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode," Rev. 2, July 1981.

---, NUREG-1150, "Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plants, Final Summary Report," December 31, 1990.

---, NUREG/CR-4627, "Generic Cost Estimates," June 1986.

---, NUREG/CR-5160, "Guidelines for the Use of the EEDB at the Sub-Component and System Level," May 1988.

---, NUREG/CR-5236, "Radiation Related Impacts for Nuclear Plant Physical Modifications," October 1989.

---, NUREG/CR-5640, "Overview and Comparison of U.S. Commercial Nuclear Power Plants," September 1990.

Nuclear Safety Analysis Center, NSAC/60, "Oconee PRA," Palo Alto, June 1984.

Russell, K. D., M. K. McKay, M. B., Stattison, N. L. Skinner, S. T. Wood, and D. M. Rasmuson, NUREG/CR-5813, "Integrated Reliability and Risk Analysis System (IRRAS) Version 4.0," Idaho National Engineering Laboratory and EG&G Idaho, Inc., January 1992.

Swain, A., and H. Guttmann, NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," Sandia National Laboratories, 1983.

Taylor, J. M., NRC Policy Issue (Notation Vote) SECY-93-167, "Regulatory Analysis Guidelines of the U. S. Nuclear Regulatory Commission," June 14, 1993.

Thadani, A., NRC, Memorandum for T. Novak and J. Olshinski, "Comparative Risk Assessment of ECCS Functional Switchover Options," April 1, 1981.

Westinghouse Electric Corporation, WCAP 13186, "An Evaluation of the Revised Transfer to Cold Leg Recirculation Procedure," January 1992.

Weston, L. M., D. W. Whitehead, N. L. Graves, NUREG/CR-4834, "Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP)," SAND-87-0719, June 1987.

10 CFR 50.46, "Acceptance criteria for emergency core cooling systems for light water nuclear power reactors," Code of Federal Regulations, January 1992.

10 CFR 50.109, "Backfitting," Code of Federal Regulations, January 1992.

Appendix A

Introduction to ECCS Switchover to Recirculation

Table of Contents

List of Figures

A.1 Normal PWR Operations

A.1.1 PWR Primary System

A Pressurized Water Reactor (PWR) generates heat in a core that is cooled and moderated by light water. The core contains fuel rods consisting of uranium oxide pellets within cylindrical Zircaloy cladding.

Heat is transferred from the reactor core by the Reactor Coolant System (RCS), which circulates through high-pressure loops (about 2200 psig). In each loop, the reactor core is the heat source and steam generators are the heat sink. Figure A.1 (NRC, NUREG/CR-5640) is a schematic of one loop of a typical RCS.

During power operation, the Steam and Power Conversion System removes heat by boiling water in the steam generators. The main turbine generators extract power from the steam to generate electricity. Waste heat is rejected through the main condenser to the ultimate heat sink, which is a body of water, the atmosphere, or both.

A.1.2 Charging Pumps

The Chemical and Volume Control System performs the RCS coolant inventory control function. Charging pumps inject coolant into the high-pressure RCS loops, as shown in Figure A-2 (NRC, NUREG/CR-5640).

A.1.3 Shutdown Cooling System

After a normal interruption of power operation, initial shutdown cooling is accomplished by using the main turbine bypass system to direct steam to the main condensers (Hot Shutdown). This is essentially the same heat transport path as is used during power operation except that the main turbine is tripped and bypassed.

After initial cooldown and depressurization, the Residual Heat Removal (RHR) System provides for post-shutdown cooling of the RCS. As illustrated in Figure A.3 (NRC, NUREG/CR-5640), the RHR system establishes a different heat transfer loop by diverting reactor coolant to the RHR heat exchangers, through which the heat can be transferred to the ultimate heat sink.

A.2 Loss-of-Coolant Accidents

A.2.1 Engineered Safety Feature Actuation System

The role of the Engineered Safety Feature Actuation System (ESFAS) is to actuate components and systems, other than a reactor scram, needed to mitigate the consequences of events that challenge normal plant operation. As illustrated in Figure A.4 (NRC, NUREG/CR-5640), the ESFAS includes provisions for manual actuation at the system level (typically from the control room) or at the actuation-train level (typically from the ESFAS output logic cabinets). A manual trip from the control room actuates all components that would be actuated by an automatic ESFAS actuation signal. A manual trip from ESFAS output logic cabinets actuates only the components that are controlled by the respective ESFAS train.

A.2.2 ECCS

Following a breach in the RCS pressure boundary, water is lost from the RCS at a rate that is determined by several factors, including break size and location. LOCAs are hypothetical accidents that would result if the rate of loss of reactor coolant exceeded the capability of the reactor coolant makeup system.

The ECCS first injects makeup water into the RCS during a LOCA and later recirculates water through the core following a LOCA to provide for long-term post-accident core cooling. In all PWRs, the ECCS includes pressurized safety injection tanks (SITs) and high- and low-pressure safety injection (HPSI and LPSI) pumps.

In most PWRs, the RHR pumps perform the LPSI function. At many plants the HPSI function is performed in whole or in part by the normal charging pumps.

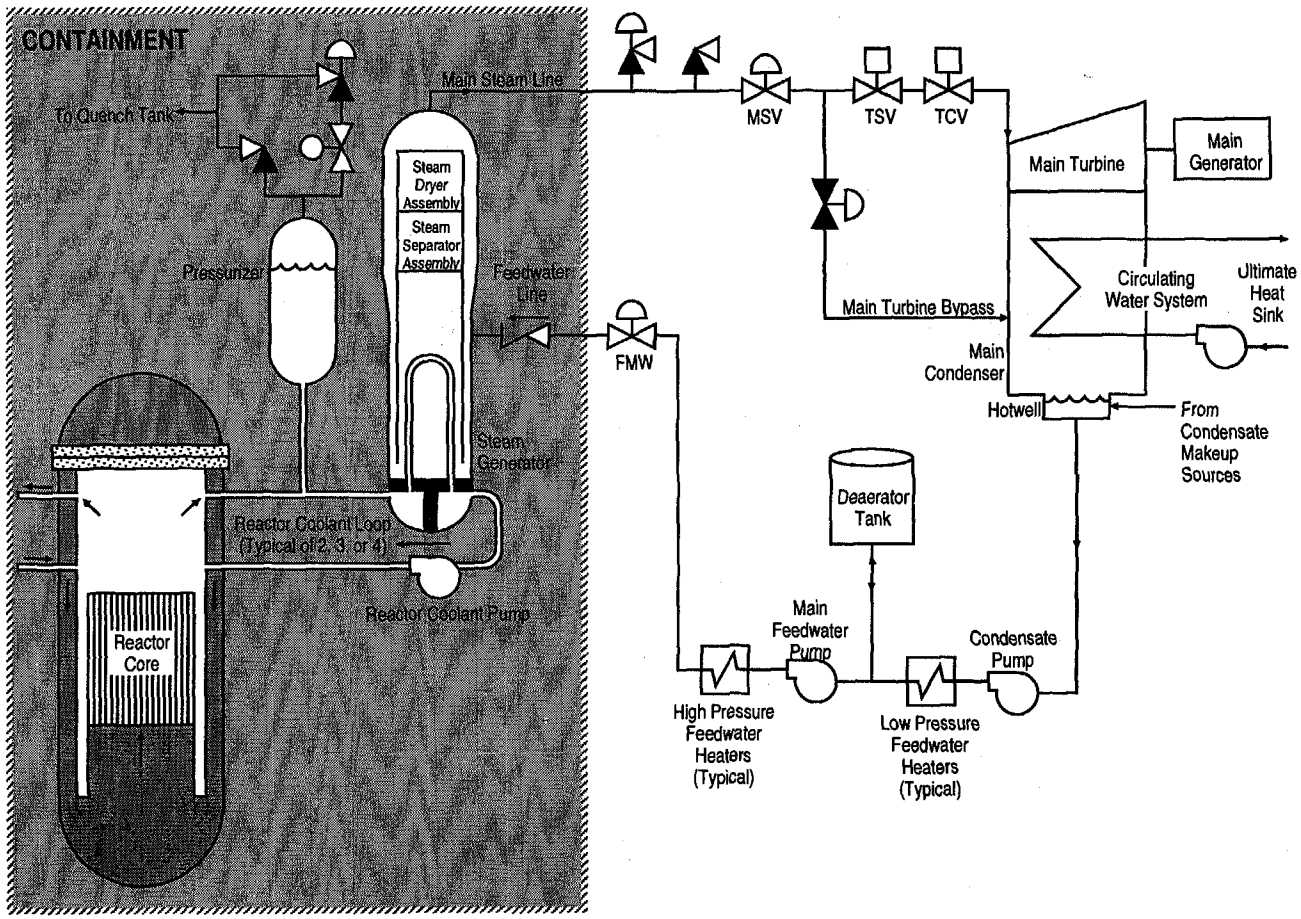

Figure A.1 Normal PWR Heat Transport Paths During Power Operation

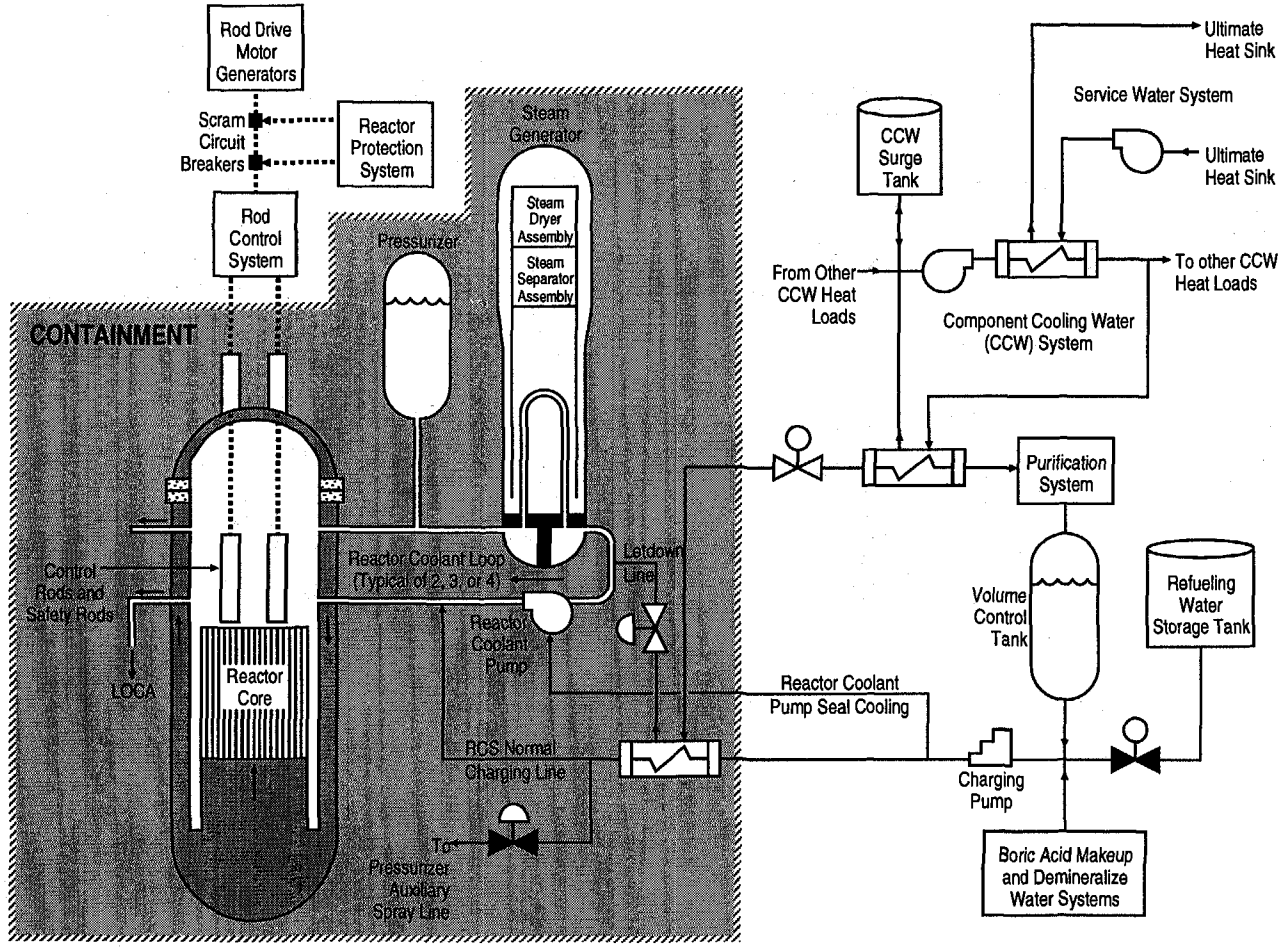

Figure A.2 PWR Reactivity Control Systems: Control Rods and the Chemical and Volume Control System

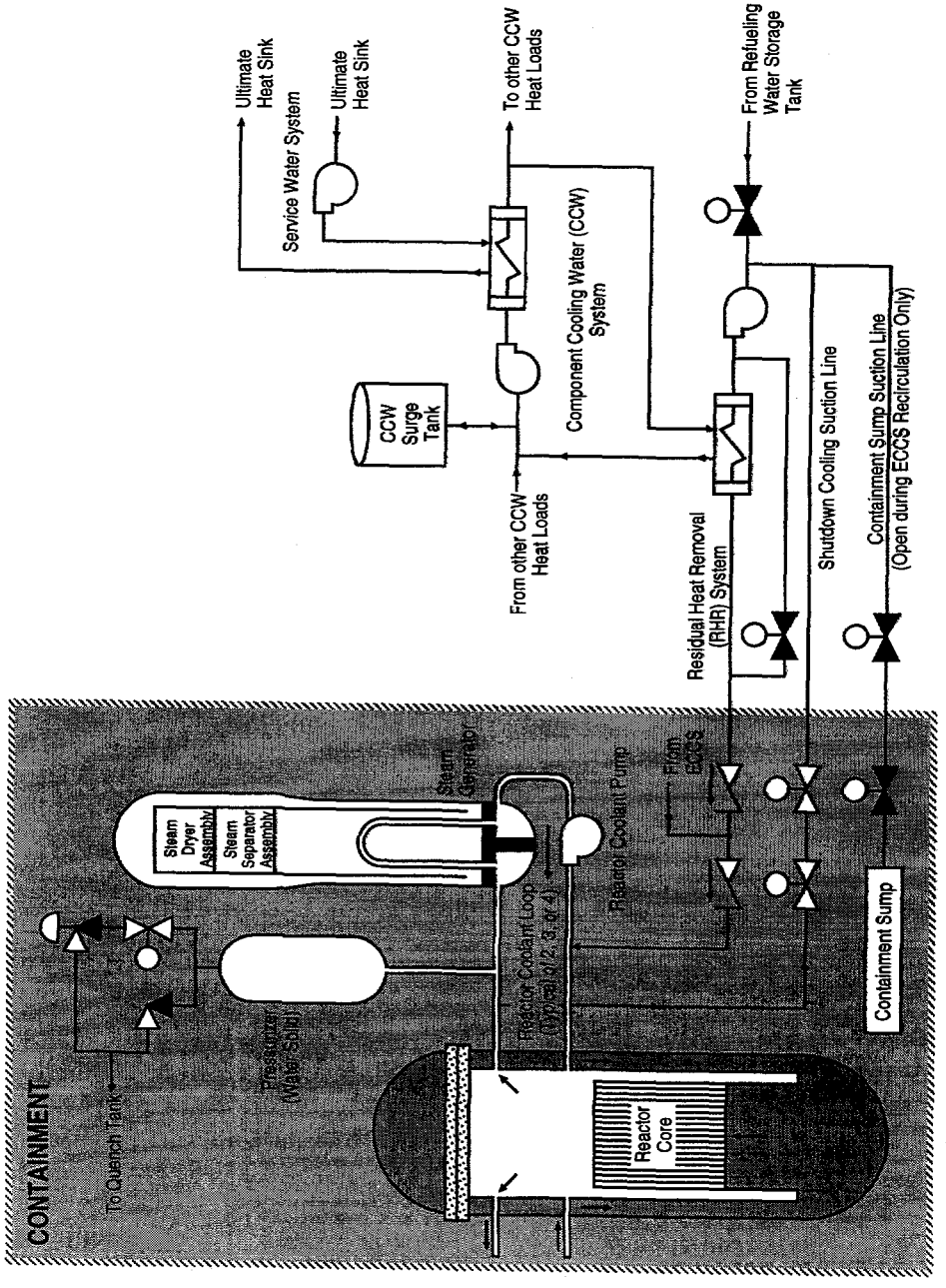

Figure A.3 Normal PWR Heat Transport Paths During Shutdown Cooling

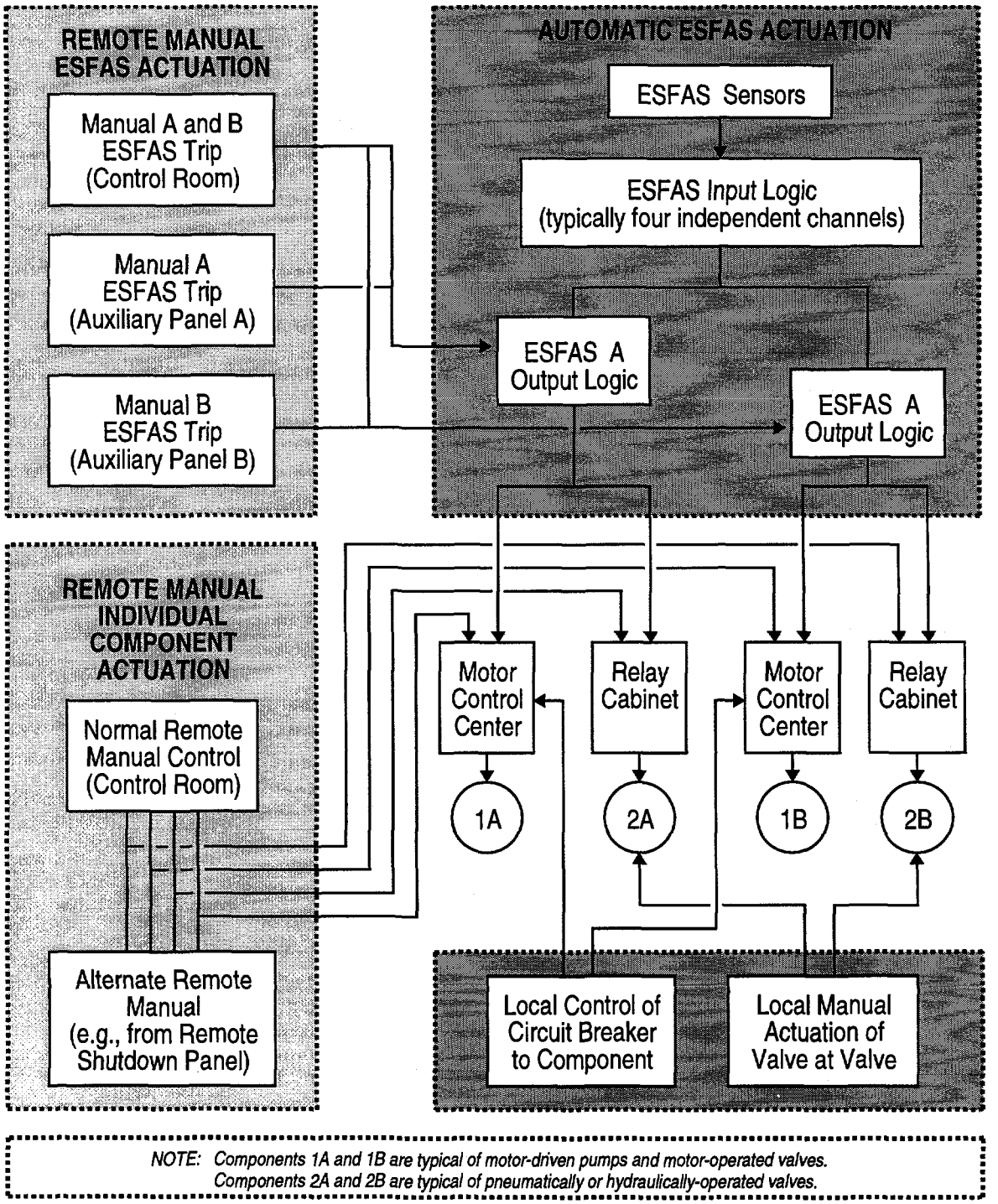

Figure A.4 Example of Actuation System Interfaces

A.2.3 ECCS Injection Phase

During the injection phase of operation following a large LOCA, the ECCS operates as an open-loop system and provides rapid injection of borated water to the RCS to ensure reactor shutdown and adequate core cooling. Following a large LOCA, the RCS is rapidly depressurized, and makeup is initially provided by the safety injection accumulators as RCS pressure drops below the accumulator pressure (650 psig). Both the HPSI and LPSI pumps are aligned to take a suction on the Refueling Water Storage Tank (RWST) and deliver makeup water to the reactor vessel. Water lost from the RCS is collected in the containment sump. The coolant injection and heat transport paths associated with large LOCA mitigation are shown in Figure A.5 (NRC, NUREG/CR-5640).

Following a small LOCA, the RCS may slowly depressurize or remain at or near normal operating pressure, preventing injection by the SITs or the LPSI pumps.

A.2.4 Containment Spray System

In most PWRs, a containment spray system initially injects water from the RWST into the containment. When the RWST has been emptied, spray pump suction is aligned to the containment sump or a separate recirculation spray system is started. The operation of the containment spray system increases the rate at which water is pumped from the RWST and therefore reduces the time that the ECCS can continue to pump from the RWST before the tank is emptied.

A.2.5 ECCS Recirculation Phase

When the RWST makeup water supply reaches a low level, the ECCS is placed in the recirculation mode of operation by aligning the suctions of the LPSI pumps to the containment sump and isolating the suction path from the RWST. In most PWR plants, the HPSI pumps cannot be aligned to take a suction directly from the containment sump. At the time recirculation is actuated, the normally dry containment sump is full of water that has collected from the RCS break and from the operation of the containment spray system. The break has contributed water that was in the RCS at the time of the accident and additional water from ECCS operation. During recirculation, water returns to the containment sump through the RCS break that caused the LOCA.

Following a large LOCA, the RCS is depressurized to the point that the LPSI pumps can provide continuous makeup to the RCS and the HPSI pumps may be stopped. Heat exchangers in the LPSI system may be used during the recirculation phase to transfer heat to the ultimate heat sink. The low-pressure ECCS recirculation loop is comparable to the RHR shutdown cooling loop with the exception that the low-pressure pumps are aligned to take a suction from the containment sump.

During a small LOCA, RCS pressure may remain high at the time that the RWST reaches the switchover level, precluding recirculation with just the LPSI pumps, which typically have a shutoff head on the order of 300 to 400 psig. In this case, 2-loop Combustion Engineering PWRs can be aligned such that the HPSI pumps take a suction on the containment sump, but most other plants establish the high-pressure recirculation flow path with the LPSI and HPSI pumps operating in tandem. In tandem operation the low-pressure pumps take a suction on the containment sump and are aligned to deliver the water to the suction of the high-pressure pumps which then inject water into the RCS. Heat exchangers in the LPSI system may be used during high-pressure recirculation to transfer heat to the ultimate heat sink.

A.3 Reference

NRC, NUREG/CR-5640, "Overview and Comparison of U.S. Commercial Nuclear Power Plants," September 1990.

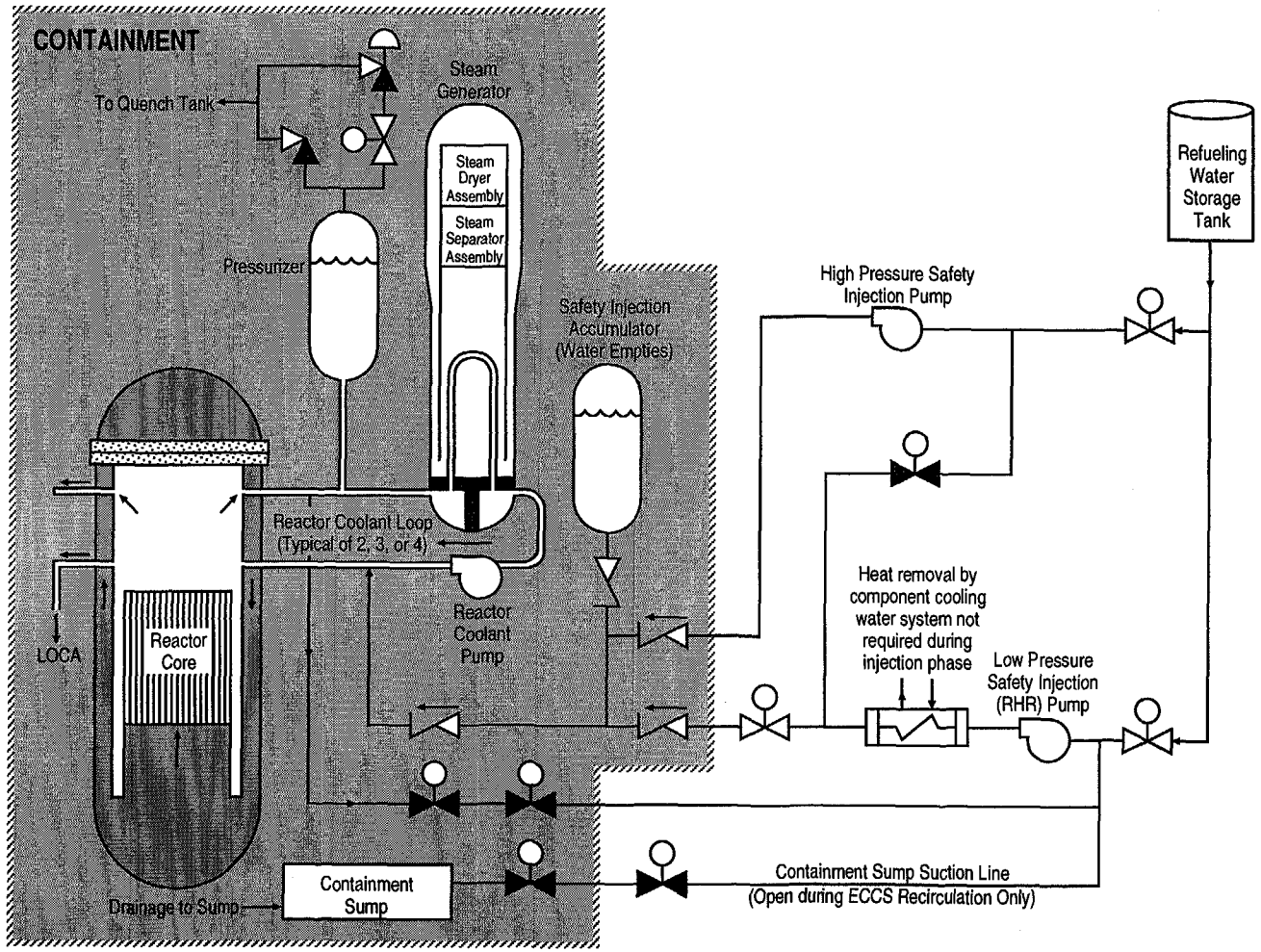

Figure A.5 ECCS Coolant Injection and Heat Transport Paths During a Large LOCA

Appendix B

Current Acceptance Criteria for ECCS Switchover Systems

Table of Contents

B.1 Success Criteria for Fully Operational ECCS

Current requirements provide that the ECCS be designed such that its calculated cooling performance following postulated LOCAs conforms to the following criteria (10 CFR 50.46):

(1) Peak Cladding Temperature (PCT). The calculated maximum fuel element cladding temperature shall not exceed 2200°F.

(2) Maximum Cladding Oxidation. The calculated total oxidation of the cladding shall nowhere exceed 0.17 times the total cladding thickness before oxidation.

(3) Maximum Hydrogen Generation. The calculated total amount of hydrogen generated from the chemical reaction of the cladding with water or steam shall not exceed 0.01 times the hypothetical amount that would be generated if all of the metal in the cladding cylinders surrounding the fuel, excluding the cladding surround the plenum volume, were to react.

(4) Coolable Geometry. Calculated changes in core geometry shall be such that the core remains amenable to cooling.

Cooling performance through switchover must be calculated for a number of postulated LOCAs sufficient to provide assurance that the most severe postulated LOCAs are calculated. Postulated LOCAs include pipe breaks up to and including the double-ended rupture of the largest pipe in the RCS. Detailed criteria for acceptable ECCS evaluation models are provided (10 CFR 50 Appendix K).

B.2 Success Criterion with a Single Failure

Current regulations state that the design of the ECCS shall assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure (10 CFR 50 Appendix A, Criterion 35). The safety function is defined to be transfer of heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts. That is, the design does not have to meet the level of cooling performance that is required of fully operational ECCS.

A single failure is defined to be an occurrence which results in the loss of capability of a component to perform its intended safety functions, including multiple failures resulting from a single occurrence. The ECCS must perform its safety function with a single failure of any active component (assuming passive components function properly). Different single failures may be limiting, depending on the particular break location and break size postulated.

B.3 Design Requirements for ECCS Switchover Control

Protection systems (including sense and command features for ECCS) are required (10 CFR 50.55a) to meet the requirements of IEEE criteria (IEEE-279) or its updates. IEEE-279 has been withdrawn and a new standard has been proposed (IEEE Std 603-1991).

IEEE-603 requires that a specific basis be established for the design of ECCS, including documentation of

(1) The points in time and the plant conditions during which manual control is allowed.

(2) The justification for permitting control subsequent to initiation solely by manual means.

(3) The range of environmental conditions imposed upon the operator during accident circumstances throughout which the manual operations shall be performed.

(4) The variables that shall be displayed for the operator to use in taking manual action.

Means shall be provided to automatically control the system except as so justified. IEEE-603 also requires that display instrumentation provided for fully manual switchover meet the requirements of IEEE Standard 497 and minimize the possibility of

ambiguous indications that could be confusing to the operator.

For new construction permits, the Standard Review Plan includes examination of the complete sequence of ECCS operation "to see that a minimum of manual action is required and, where manual action is used, a sufficient time (greater than 20 minutes) is available for the operator to respond" (NRC, NUREG-0800, Sec. 6.3).

The Standard Review Plan includes a technical position that considers ECCS switchover acceptance criteria in comparison with the requirements for protection system initiation (NRC, NUREG-0800, App. 7-A, ICSB 20). Automatic transfer to the recirculation mode is stated to be preferable. A design that provides manual actuation at the system level, while not ideal, is considered to be sufficient and to satisfy the intent of IEEE-279 provided that

- adequate instrumentation and information display are available to the operator so that he can make the correct decision at the correct time and
- in case of operator error, there are sufficient time and information available so that the operator can correct the error with acceptable consequences.

B.4 References

IEEE Power Engineering Society, IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," December 31, 1991.

Institute for Electrical and Electronics Engineers, IEEE-279, "Criteria for Protection Systems for Nuclear Power Generating Stations," 1971.

NRC, NUREG-0800, Rev. 2 "Standard Review Plan," Section 6.3, "Emergency Core Cooling System," April 1984.

NRC, NUREG-0800, "Standard Review Plan," Appendix 7-A, "Branch Technical Positions (ICSB)," Branch Technical Position ICSB 20, "Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode," Rev. 2, July 1981.

10 CFR 50 Appendix A, Criterion 35, "Emergency Core Cooling," Code of Federal Regulations, January 1992.

10 CFR 50 Appendix K, "ECCS Evaluation Models," Code of Federal Regulations, January 1992.

10 CFR 50.46, " Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors," Code of Federal Regulations, January 1992.

10 CFR 50.55a, "Codes and Standards," Code of Federal Regulations, January 1992.

Appendix C

Status of ECCS Switchover Control at Operating PWRs

Table of Contents

List of Tables

C.1 Extent of ECCS Switchover Automation

Generic Issue No. 24, "Automatic ECCS Switchover to Recirculation" includes the question of whether there is a supportable need for modification to manual, semiautomatic or automatic systems in PWRs currently operating. "Supportable" is in the context of the backfit rule and relevant cost/benefit guidance. Cost/benefit analyses of any potential requirement needs an estimate of the number of plants that would be affected.

There are two types of modification that are potentially supportable. The type that is the subject of the present study is an improvement to a manual system, such as introducing some degree of automation. The updated FSARs available at the NRC Public Document Room were reviewed for information as to which plants have manual, semiautomatic, or automatic switchover of ECCS to cold leg recirculation. There are 68 PWRs in commercial operation in the United States at this time.

The operating PWRs that have manual switchover of ECCS to cold-leg recirculation were identified by elimination. A plant was considered to have a semiautomatic system, and was included in Table C.1 or C.2, if the switchover of the low-pressure system requires no operator intervention other than actuation. Tables C.3 and C.4 list the plants that were considered to have automatic switchover because neither low- nor high-pressure switchover requires operator intervention other than actuation. The remaining plants were taken to have manual switchover and are entered in Tables C.5 and C.6. The updated FSAR for Salem does not make any distinction between Units 1 and 2. However the EOPs for ECCS switchover at these plants determine that Unit 1 is manual and Unit 2 is semiautomatic. This highlights the uncertainty in Tables C.1 through C.6, which are limited to readily available public information.

Table C.1 Operating PWRs with Semiautomatic ECCS Switchover and No Risk From Spurious Actuation (per plant visit or description in updated SAR)

Plant	NSSS	NRC Docket	Source
Salem 2	W	50-311/P	Plant Visit
Beaver Valley 2	W	50-412/P	USAR, 5/93

Table C.2 Operating PWRs with Semiautomatic ECCS Switchover (per description in updated SAR) that Were Not Included in Table C.1

Plant	NSSS	NRC Docket	Source
McGuire 1	W	50-369/P	USAR, 10/92
McGuire 2	W	50-370/P	USAR, 10/92
Catawba 1	W	50-413/P	USAR, 4/93
Catawba 2	W	50-414/P	USAR, 4/93
Sequoyah 1	W	50-327/P	USAR, 11/92
Sequoyah 2	W	50-328/P	USAR, 11/92
Callaway	W	50-483/P	USAR, 6/92
Wolf Creek	W	50-482/P	USAR, 3/93

Table C.3 Operating PWRs with Automatic ECCS Switchover and No Risk From Spurious Actuation (per description in updated SAR)

Plant	NSSS	NRC Docket	Source
Surry 1	W	50-280/P	USAR, 7/93
Surry 2	W	50-281/P	USAR, 7/93
Beaver Valley 1	W	50-334/P	USAR, 7/93
South Texas 1	W	50-498/P	USAR, 9/93
South Texas 2	W	50-499/P	USAR, 9/93
North Anna 1	W	50-338/P	USAR, 7/92
North Anna 2	W	50-339/P	USAR, 7/92

C.2 Potential Vulnerability to Spurious Switchover Actuation

To avoid duplication of effort, the review of updated FSARs also captured information relevant to another type of potentially supportable modification covered by GSI-24. This is a modification to avoid a spurious switchover actuation during shutdown that would interrupt the Residual Heat Removal (RHR) system.

Should a spurious ECCS recirculation signal occur in a plant that uses RHR for low pressure ECCS injection, the running RHR pump would be realigned to an empty containment sump, and the pump could overheat unless tripped. Even if the pump is tripped before being damaged, air has accumulated at piping/pump high points and could lead to problems if the pump is restarted with a water source. Other RHR trains may not be readily available because maintenance is scheduled during shutdown.

Table C.4 Operating PWRs with Automatic ECCS Switchover (per updated SAR) that Were Not Included in Table C.3

Plant	NSSS	NRC Docket	Source
Maine Yankee	C-E	50-309/P	IPE
Fort Calhoun	C-E	50-285/P	USAR, 7/93
ANO 2	C-E	50-368/P	USAR, 7/93
Calvert Cliffs 1	C-E	50-317/P	USAR, 3/93
Calvert Cliffs 2	C-E	50-318/P	USAR, 3/93
Millstone 2	C-E	50-336/P	USAR, 6/93
Palo Verde 1	C-E	50-528/P	IPE
Palo Verde 2	C-E	50-529/P	IPE
Palo Verde 3	C-E	50-530/P	IPE
Palisades	C-E	50-255/P	USAR, 4/93
St. Lucie 2	C-E	50-389/P	USAR[1], 9/93
Waterford 3	C-E	50-382/P	USAR[1], 12/92
St. Lucie 1	C-E	50-335/P	USAR[1], 7/92
San Onofre 2	C-E	50-361/P	USAR[1], 2/93
San Onofre 3	C-E	50-362/P	USAR[1], 2/93

[1]The low pressure pumps are not used for recirculation, therefore the automatic sequence does realign these pumps.

In cold shutdown the containment can be open. The time to close an open containment depends on whether or not the large, heavy equipment hatch is open. If it is open, the time to isolate containment is long. Without offsite power, the hatch probably cannot be moved.

The consequences of a loss of RHR depend upon many factors, including

- the elapsed time since shutdown,
- the time required to recover RHR,
- whether or not the contents of the RWST are injected,
- whether the containment is isolated before core damage, and
- the type of containment.

Preliminary results are available from an NRC-sponsored study of shutdown risk at a representative PWR. The plant studied was Surry, which has separate RHR and low pressure injection pumps. The draft report states that a spurious recirculation transfer signal will line up ECCS into a recirculation mode but will not affect RHR shutdown cooling.

Table C.1, C.3, and C.5 identify those PWRs that, according to readily available public information, have negligible risk of losing Residual Heat Removal as a result of spurious switchover actuation during cold shutdown.

If the plant is semiautomatic or automatic, actuation may be automatic or operator-dependent. Spurious actuation during shutdown can be eliminated as a problem if any of the following criteria are met:

- low-pressure ECCS has its own pumps, rather than using the RHR pumps,
- actuation in normal operation requires an operator action, or
- switchover is specifically disabled during shutdown operation.

There are 7 automatic plants and 1 semiautomatic plant where spurious actuation of the switchover function can be ruled out. In these plants low-pressure ECCS has its own pumps and does not rely on the residual heat removal pumps. Another semiautomatic plant can be ruled out because the system does not begin switchover until the operator confirms that the RWST has reached the appropriate level. These eight plants are all Westinghouse plants that came into service from 1977 through 1988.

There are 8 Westinghouse plants which have semiautomatic switchover where spurious actuation of the switchover function could not be ruled out. These plants all use the RHR pumps for the low pressure ECCS function.

In the 15 C-E plants the high-pressure pumps automatically initiate and complete the switchover process. However, the Recirculation Actuation Signal trips the low pressure pumps. The low pressure pumps are not used in the recirculation mode of the ECCS. The low pressure pumps are used for the shutdown cooling function. What effect a spurious signal to switchover would have on the shutdown cooling capability cannot be determined without plant specific operating procedures during shutdown.

There are 9 Westinghouse plants which have manual switchover procedures according to our criteria (part of the low-pressure switchover is manual), but because the system automatically aligns the suction of the RHR pumps to the containment recirculation sump, spurious actuation of the system cannot be ruled out. All of these plants use the RHR pumps for the low pressure ECCS function.

Table C.5 Operating PWRs with Manual ECCS Switchover and No Risk From Spurious Actuation (per description in IPE submittal or updated SAR)

Plant	NSSS	Contain-ment Type	NRC Docket	Year License Expires	Source
Robinson 2	W	Dry	50-261/P	2007	USAR, 2/93
Point Beach 1	W	Dry	50-266/P	2010	USAR, 6/93
Point Beach 2	W	Dry	50-301/P	2013	USAR, 6/93
Turkey Point 3	W	Dry	50-250/P	2007	USAR, 7/92
Turkey Point 4	W	Dry	50-251/P	2007	USAR, 7/92
Oconee 1	B&W	Dry	50-269/P	2013	IPE
Oconee 2	B&W	Dry	50-270/P	2013	IPE
Oconee 3	B&W	Dry	50-287/P	2014	IPE
Indian Point 2	W	Dry	50-247/P	2013	USAR, 6/93
Indian Point 3	W	Dry	50-286/P	2009	USAR, 7/93
Zion 1	W	Dry	50-295/P	2008	USAR, 8/93
Zion 2	W	Dry	50-304/P	2008	USAR, 8/93
Kewaunee	W	Dry	50-305/P	2008	USAR, 7/93
Prairie Island 1	W	Dry	50-282/P	2013	USAR, 9/93
Prairie Island 2	W	Dry	50-306/P	2014	USAR. 9/93
Three Mile Island 1	B&W	Dry	50-289/P	2008	USAR, 7/92
ANO 1	B&W	Dry	50-313/P	2008	USAR, 7/93
Cook 1	W	Ice Cond.	50-315/P	2009	USAR, 7/93
Cook 2	W	Ice Cond.	50-316/P	2009	USAR, 7/93
Millstone 3	W	Sub-Atm.	50-423/P	2025	USAR[2], 6/93
Haddam Neck	W	Dry	50-213/P	2004	USAR[1], 6/92
Crystal River 3	B&W	Dry	50-302/P	2016	USAR, 7/93
Diablo Canyon 1	W	Dry	50-275/P	2008	USAR[2], 9/92
Diablo Canyon 2	W	Dry	50-323/P	2010	USAR[2], 9/92
Salem 1	W	Dry	50-272/P	2008	USAR, 7/92
Ginna	W	Dry	50-244/P	2006	USAR, 12/92
Davis Besse	B&W	Dry	50-364/P	2011	USAR, 10/92

[1]The RHR suction is automatically aligned to the sump, but not the complete switchover of the RHR pumps.
[2]The RHR pumps stop automatically on a low-low level signal from the RWST.

Table C.6 Operating PWRs with Manual ECCS Switchover (per description in updated SAR) Not Included in Table C.5

Plant	NSSS	Containment Type	NRC Docket	Year License Expires	Source
Braidwood 1	W	Dry	50-456/P	2026	USAR[1], 12/92
Braidwood 2	W	Dry	50-457/P	2027	USAR[1], 12/92
Byron 1	W	Dry	50-454/P	2024	USAR[1], 12/92
Byron 2	W	Dry	50-455/P	2026	USAR, 12/92
Summer	W	Dry	50-395/P	2023	USAR[1], 10/92
Farley 1	W	Dry	50-348/P	2012	USAR[1], 6/93
Farley 2	W	Dry	50-364/P	2012	USAR[1], 6/93
Vogtle 1	W	Dry	50-424/P	2027	USAR[1], 12/92
Shearon Harris	W	Dry	50-400/P	2026	USAR[1], 6/93

[1]The RHR suction is automatically aligned to the sump, but not the complete switchover of the RHR pumps.

Appendix D

Evaluation of HRA Methods

Table of Contents

D.1 Previous Comparative Evaluations

The RMIEP study (Haney and Blackman) evaluated twelve methods of human reliability assessment. This appendix evaluates the twelve methods for potential application in the GSI-24 HRA.

The RMIEP document presented a rating scale, based on six criteria, with rankings of 1 to 4 on each criterion, which was used in evaluating the methods. The six criteria were:

Availability of Method
Availability of Data
History of Application
Type of Quantification
Process
Traceability

On each of the criteria, a rating of 1 indicated the most desirable quality, although on some of the criteria additional ratings, such as "1,2" were desirable. For example, the ratings for Type of Quantification were:

1 Point Estimate
2 Distribution
3 Semiquantitative Ranking
4 Qualitative

Thus, a rating of both 1 and 2 is superior to 1 alone (that is, distributions as well as point estimates are available). If a rating of 4 was assigned (qualitative only) the method was dropped from consideration for further evaluation.

For this reason, and others, an original set of 20 methods was reduced to 12. The 12 remaining methods were:

1. Confusion Matrix (Potash and Stewart)
2. Dougherty
3. Expert estimation (Comer and Seaver)
4. Fullwood and Gilbert
5. Human Cognitive Reliability Model (Hannaman and Spurgin)
6. Operator Action Tree (OAT) (Hall and Fragola)
7. Sandia Recovery Model (SRM) (Weston and Whitehead)
8. Simulator Data (Beare and Dorris)
9. Success Likelihood Index Method (SLIM) (Embrey)
10. Socio-Technical Assessment of Human Reliability (STAHR) (Phillips and Humphreys)
11. Technique for Human Error Rate Prediction (THERP) (Swain and Guttmann)
12. Woods

Shortly after the RMIEP study was published a book appeared evaluating a number of Human Reliability Analysis methods (Swain, 1989).

The Swain evaluations are based on different, more detailed criteria than those used in RMIEP. Swain defined three major criteria for evaluating HRA methods: Usefulness, Acceptability, and Practicality. The three major criteria are comprised of a number of subcriteria, each described in detail. The final rating of each method is based on "PASS/FAIL" evaluations assigned to the three major criteria.

Fourteen methods were evaluated, including two authored by Swain. The authors of the other twelve methods were invited to participate in the ratings. With two exceptions, all responded. In all but four instances, someone in addition to Swain participated in the rating.

Of the twelve methods evaluated by RMIEP, six were also evaluated by the Swain raters:

Method	Usefulness	Accept-ability	Practi-cality
CONF.MATRIX	FAIL	PASS	PASS
HCR	FAIL	PASS	PASS
OAT	FAIL	PASS	PASS
SLIM	FAIL	FAIL	FAIL
STAHR	FAIL	FAIL	FAIL
THERP	PASS	PASS	PASS

With the exception of THERP, none of the six methods received a unanimous "PASS" on all three criteria. Since Swain was using criteria other than those used in RMIEP, differences in overall ratings are understandable. There is also the possibility that the Swain raters were more stringent in their ratings.

Although both RMIEP and Swain present guides to evaluating HRA methods, the evaluation in this Appendix is independent. The GSI-24 study needs

reliable and readily available Human Reliability methodology and data.

Several of the RMIEP methods rely upon various psychological scaling techniques, which require estimates elicited from groups of people of various disciplines. These methods are referred to as "Expert Judgment" methods.

Expert Judgment methods involve estimates derived from a number of subject-matter experts. The estimates are treated by various statistical techniques (psychological scaling) to arrive at consensus estimates of probabilities. Psychological scaling methods yield useful estimates of error probabilities and success probabilities, but they have the disadvantage of requiring numbers of subject-matter experts, and they require considerable time and effort. Typically, they involve more effort than other methods to derive HEPs, and there is less certainty in their error estimates than in HEPs derived from more objective methods. The following methods are Expert Judgment methods, and therefore not suitable for use in this GSI-24 HRA:

CONFUSION MATRIX
EXPERT ESTIMATION
SLIM
STAHR

D.2 Evaluation of Candidate Methods

This section evaluates the remaining eight methods for potential value in the GSI-24 HRA. Methods are considered for their applicability to rule-based procedures, where time is not a consideration, and to cognitive, knowledge-based behavior. To be of use in the GSI-24 study, a method must be supported by validated values for its parameters.

D.2.1 Dougherty

This technique (Dougherty), was described somewhat scantly in RMIEP. It is an internal report of the Technology for Energy Corporation, Knoxville, Tennessee. Based on the RMIEP description, it seems that it depends upon other methods for error probabilities. It does not appear to offer any advantages over the other methods, and in view of its relative unavailability, it is not used in this GSI-24 HRA.

D.2.2 Fullwood and Gilbert

This technique was presented in 1976 (Fullwood and Gilbert). Thus, it is somewhat dated. However, Fullwood and Gilbert had some novel concepts of stress, which are considered in evaluating stress as a performance shaping factor.

D.2.3 Human Cognitive Reliability Model

The Human Cognitive Reliability Model (HCR) (Hannaman and Spurgin), presents graphs of error probabilities (called "non responses") versus time, and treats the various levels of cognitive behavior (knowledge-based, skill-based and rule-based). It is primarily applicable to the detection and diagnosis phases of abnormal events. The HCR does not address time-dependent HEPs for post-diagnosis actions; users must obtain such data from other sources. Although HCR is not a "stand-alone" HRA, the time-response correlation data is useful for this GSI-24 HRA.

D.2.4 Operator Action Tree

The Operator Action Tree (OAT) (Hall and Fragola), is similar to the HCR in that it is also based on a Time Reliability Correlation (TRC), and also is used primarily for estimating the likelihood of success in diagnosing abnormal events. OAT stresses the importance of time versus error probability, and presents a simple formula for computing the amount of time available for "thinking" as a function of total time available and time required to implement required actions. The graph of time-reliability is similar to the one in the HRA Handbook. The example of an application of OAT in RMIEP indicates that time is the primary criterion of success. The action trees include time estimates for every action required, the total activity time is subtracted from the total time available, yielding the time allowed for thinking. This figure is applied to the TRC graph to obtain the probability of success.

D.2.5 The Sandia Recovery Model (SRM)

The SRM (Weston and Whitehead).is similar to other methods that use a time-reliability curve to relate error probability to time. However, it is ground-breaking in that all the data are hard data, as all data were collected in simulator runs. Ten classes of recovery action were studied in simulator exercises, and success probability curves for the ten exercises were prepared. The sample size of each recovery class ranged from 3 through 83, with a median size of 20. The ten classes of recovery action are described in general terms, so that the data collected can be extrapolated to similar Nuclear Power Plants.

The SRM presents ten time-reliability curves, with tabled values of success probabilities, including the upper and lower 95% confidence limits.

This technique promises to be much more valuable than other techniques based on time-reliability correlations, as the data were obtained in simulators, a situation which most closely corresponds to a real-life situation. Previous methods using TRCs derived the TRCs on the basis of expert judgment, and were necessarily conservative. Also, such estimates could not provide confidence limits based on data; the analyst had to use his judgment to estimate upper and lower bounds, based on a study of the salient performance shaping factors.

D.2.6 Simulator Data

Simulators currently are our most useful source of "hard" data on operator performance and error probabilities. In the simulator the trainees can undergo any number of situations that occur only rarely in real life, and thus can be trained in the responses to such situations. Also, if the simulator is arranged for data collection, it provides data on the time required to respond to a situation, and the types and frequencies of errors that are committed. The simulator study cited in RMIEP (Beare and Dorris), was conducted for the purpose of obtaining hard data to compare with HEPs in the HRA Handbook (Swain and Guttmann).

Although simulator data are probably the most valid currently available, the use of a simulator does not constitute an HRA method, and is not regarded as such in this evaluation. Simulators are a useful source of data on operator performance, and the data from simulator studies is incorporated in this GSI-24 HRA as available and appropriate.

D.2.7 Woods

Woods offers another technique for relating cognitive performance to the time available to perform the task (Woods). This seems to be a variant of the TRC approach, with some modifications. It is not of interest to this GSI-24 HRA.

D.2.8 Technique for Human Error Rate Prediction (THERP)

THERP is the HRA method described in the HRA Handbook (Swain and Guttmann) and the two terms (THERP and HRA Handbook) are often used synonymously.

Briefly, THERP is "a method to predict human error probabilities and to evaluate the degradation of a man-machine system likely to be caused by human errors alone or in connection with equipment functioning, operational procedures and practices, or other systems and human characteristics that influence system behavior" (Swain and Guttmann, p.5-3). THERP is a comprehensive methodology, using a detailed analytical approach to provide a numerical basis for Human Reliability Assessments. The technique was developed by A. D. Swain at Sandia National Laboratories in 1961 to evaluate the reliability of military systems and components. It was the first formalized method developed for the purpose of assessing human reliability. It was found to be useful and accurate, and was used regularly in the reliability assessments of weapon systems. THERP was used in the first comprehensive PRA of a nuclear power plant, known as WASH-1400 (NRC, NUREG-75/014).

The HRA Handbook was prepared at the behest of the NRC. It includes a detailed description of the THERP methodology, as it has been refined over the years. To provide the latest and most useful error data, a comprehensive review of all available human error data was completed, and a detailed data base of human error probabilities was assembled for application in HRAs. The HRA Handbook includes detailed guides for the use of THERP and the application of Performance Shaping Factors (PSFs)

in selecting Human Error Probabilities (HEPs) from the data bank. A draft version was published in 1980, and was distributed widely for comment and criticism. A large number of the recipients responded, suggesting areas that required elaboration, mentioning shortcomings, etc. The comments and criticisms were evaluated, and the draft HRA Handbook was rewritten, incorporating corrections as required. The final, complete version of the HRA Handbook was published in 1983, and has been in wide use since then.

The HRA Handbook presents a complete, stand-alone method of Human Reliability Analysis, describing Task Analysis, the preparation of event trees, and the modifications of Basic Human Error Probabilities (BHEPs) due to Performance Shaping Factors (PSFs) likely to be encountered in the work situation. It includes methods for considering the effects of different levels of stress, as well as the effects of different levels of dependence (coupling) between individuals and between actions. It also presents the basic version of the time-reliability correlation that has been used in other HRA approaches, and includes an extensive data-base of HEPs for use in conducting HRAs. A number of the HEPs were verified with data from the simulator study (Beare and Dorris).

The HRA Handbook has probably been used more extensively than any other HRA method available, and a number of the other HRA methods rely upon the HRA Handbook to supplement their basic approaches.

Although the HRA Handbook was published in August 1983, it is not a static document. When the final draft was prepared, the NRC stipulated that it be printed in loose-leaf format, as it was anticipated that changes would be effected with the passage of time. In 1987 the senior author of the HRA Handbook prepared NUREG/CR-4772 (Swain, 1987), which contains a simplified and modified version of the HRA Handbook methodology. Appendix C of that reference lists a number of corrections to the HRA Handbook, and Table 3-3 in the Swain book lists the sections of NUREG/CR-4772 that update the HRA Handbook.

Another data bank of error probabilities has been compiled by the Idaho National Engineering Laboratories (Gertman and Gilmore). This enterprise is ongoing, gathering new data as it becomes available and integrating it into the data bank. That data will be consulted as applicable.

D.3 Conclusions

Rule-based procedures are the principal focus of the THERP method, which is commonly used in NRC-sponsored PRAs. This approach is considered appropriate by the HRA community for those failures where the pace is not a major factor. Therefore, THERP is the clear choice for use in this study for errors of omission or commission while the operator is following a written procedure.

Research is continuing to develop improved models of mistake rates for knowledge-based behavior. However, no new working HRA models are expected in the near future. Meanwhile, the most widely used methods for estimating the probabilities of mistakes in knowledge-based behavior use time/reliability correlations. Any of these methods can be used in the post-LOCA phase. However, the most credible one available to date is the Sandia Recovery Model, which is based on relatively "hard" data obtained in simulator exercises, and that model is used in this study for diagnosis.

D.4 References

Beare, A. N., R. E. Dorris, C. R. Bovell, D. S. Crowe, and E. J. Kozinsky, NUREG/CR-3309, "A Simulator Based Study of Human Errors in Nuclear Power Plant Control Room Tasks," 1983.

Comer, K., D. A. Seaver, W. G. Stillwell, and C. C. Gaddy, NUREG/CR-3688, "General Human Reliability Estimates Using Expert Judgment," 1984.

Dougherty, E. M., "Modeling and Quantifying Operator Reliability in Nuclear Power Plants," TEC Internal Report, Technology for Energy Corporation, Knoxville, Tennessee.

Embrey, D. E., NUREG/CR-2986, "The Use of Performance Shaping Factors and Quantified Expert Judgment in the Evaluation of Human Reliability: An Initial Appraisal," 1983.

Fullwood, R. R., and K. J. Gilbert, "An Assessment of the Impact of Human Factors on the Operations of the CRBR SCRS," 1976.

Gertman, D. I., W. E. Gilmore, W. J. Galyean, M. R. Groh, C. D. Gentillon, and B. G. Gilbert, NUREG/CR-4639, "Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR) Volume 1: Summary Description," February 1988.

Hall, R. E., J. Fragola, and J. Wreathall, NUREG/CR-3010, "Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation," 1982.

Haney, L. N., H. S. Blackman, B. J. Bell, S. E. Rose, D. J. Hesse, L. A. Minton, and J. P. Jenkins, NUREG/CR-4835, "Comparison and Application of Quantitative Human Reliability Analysis Methods for the Risk Methods Integration and Evaluation Program (RMIEP)," January 1989.

Hannaman, G. W., A. J. Spurgin, and Y. D. Lukic, "Human Cognitive Reliability Model for PRA Analysis," NUS 4531, Electric Power Research Institute, 1984.

NUREG-75/014, WASH-1400, "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Main Report; Appendix II - Fault Trees; and Appendix III - Failure Data, October, 1975 .

Potash, L. M., M. Stewart, P. E. Dietz, C. M. Lewis, and E. M. Dougherty, "Experience in Integrating the Operator Contributions in the PRA of Actual Operating Plants," 1981 ANS/END Topical Meeting on Probabilistic Risk Assessment, Port Chester, N.Y., American Nuclear Society, LaGrange, Illinois.

Phillips, L. D., P. Humphreys, D. E. Embrey, and D. L. Selby, NUREG/CR-4183-V2, "A Socio-Technical Approach to Assessing Human Reliability (STAHR)," Appendix C, pp. 449-478.

Swain, A. D. NUREG/CR-4772, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," February 1987.

Swain, A. D., "Comparative Evaluation of Methods of Human Reliability Analysis," Gesselschaft fur Reactorsicherheit (GRS) mbh, GRS-71, April 1989.

Swain, A. D., and H. E. Guttmann, NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," 1983.

Weston, L. M., D. W. Whitehead, and N. L. Graves, NUREG/CR-4834, "Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP), Volume 1: Development of the Data-Based Method," June 1987.

Woods, D. D., "Assessment of Models of Cognitive Behavior in NPPs: I. Bounding the Assessment," in Minutes of Workshop on Modeling Cognitive Behavior Important to NPP Safety, available from Westinghouse Electric Corporation, Research and Development Center. Sponsored by USNRC, Washington, D.C., 1986.

Appendix E

Independent Review of Evaluation of HRA Methods

Table of Contents

List of Tables

E.1 Review by John Wreathall

I find the evaluation lacks currency and independence of conclusions. The evaluation is based principally on a survey of HRA methods performed by Dr. Swain under sponsorship of GRS. That survey seemed to be constructed to reflect the fact that the method rated most highly was that developed by the survey's author. This is not intended to reflect a deliberate intent of its author, but to observe that any subsequent survey of methods by a developer will reflect some of the biases that led to his methodological approach in the first place. All analysts have such biases and any survey in such circumstances must be considered appropriately. Incidentally, that survey (or any other) has not been influential in changing the selection or use of HRA methods.

The second criticism is that the selection does not recognize the thinking in the HRA field in the last 5 years as to the psychology of human errors and the relationship to the selection of HRA methods. While this is a field still evolving, work by the psychological community on the issue of error mechanisms and types has clarified the relationship of HRA methods to "real-world" risks. I enclose a text I have drafted for your review that describes what I would now expect to see in a discussion of the selection of HRA methods. Please advise me if this is of use or if any changes are required.

If necessary, a more extensive evaluation of alternative HRA methods could be added, but I am not sure the additional effort would be worth the cost. (I think the latest count of potential HRA methods is about 25; as part of an IEEE Working Group on HRA, we are logging methods prior to a wide-scale review along the lines of the attachment.)

E.2 Attachment from John Wreathall Entitled "Selection of HRA Methods"

E.2.1 Introduction

To date, several human reliability analysis (HRA) methods have been developed and applied in nuclear power plant probabilistic risk assessments (PRAs) in the USA, Canada, Europe, and Asia. In a relatively recent survey, Dougherty[1] identified 13 different HRA techniques used in power-plant PRAs. These methods vary from those using the single parameter of time available for actions as an overall basis for reliability estimation to those requiring detailed task analyses of each individual action. Some methods provide an extensive database for quantification; others provide rules for soliciting expert opinions as the basis. Not surprisingly, these methods can give diverse estimates when applied blindly to common scenarios, as was the case in European Community's HRA Benchmark Exercise[2] It is therefore important that the type of method be selected appropriately for the kinds of HRA problems being evaluated.

E.2.2 Framework for Selection of HRA Methods

Before providing the framework for selecting appropriate HRA techniques, it is necessary to define some terms to provide a common basis for relating the concepts in one technical discipline to those in another. For example, terms like "human error" have significantly different connotations in the fields of psychology, HRA and PRA, and power plant operations.

E.2.2.1 Human Errors and Safety

The term "human error" is one used imprecisely in discussions of human performance and human reliability. Conferences have held in attempts to define this term (for example, the 1983 NATO meeting in Bellagio, Italy). Yet little firm progress has been made. For example, the definition resulting from the NATO meeting was: *"If there is general agreement that an actor, Z, should have done other than what Z did, Z has committed an error".*[3]

While it is often understood in engineering studies to describe an occasion when some human action (or lack of action) led to an unsafe plant condition, the term can have the implication that the person involved is to be blamed. However, in most cases these "errors" are the product of a chain of circumstances that led up to an individual being misled or inadvertently directed into performing the "wrong thing". This position is supported by the evaluations of operational events important to safety, such as the evaluations by INEL in support of NRC AEOD.[4] Culpability may well be

distributed throughout the chain of circumstances, or there may be no blame due to anyone.

In order to neutralize the implication of culpability, the term "unsafe act" has been proposed[5] as the working term for the subject of concern in PRAs. An unsafe act is a human action (or omission of an action) that unintentionally places the plant in a less safe condition (in terms of its risk to the public or other safety criterion). An action that intended harm would be sabotage. Hence the two aspects of concern with unsafe acts are: (1) lack of intentional harm, and (2) adverse consequences to safety. In PRA, it is the event-sequence models that define the context of adverse consequences.

Not all "errors" are unsafe acts. Errors while operating systems that are error-tolerant or errors followed by prompt recovery result in no adverse consequences to safety. Errors while operating systems that have no connection to safety again do not lead to unsafe consequences.

E.2.2.2 Types of Unsafe Act

Slips, lapses, mistakes and circumventions are different types of unsafe act. They are considered to result from incorrect or inappropriate human work-related processes, such as task planning or task execution. Figure E.1 summarizes this scheme.

Slips and Lapses

Slips and lapses are unintended deviations from a planned sequence of actions. The plan may (or may not) have been good but "errors" were made in carrying it out. Slips are potentially observable as externalized actions; for example, as slips of the hand, slips of the tongue, slips of the pen, and so on. In a nuclear plant setting, slips would include the inadvertent selection of the adjacent pump or valve control on a large control panel, or transposing two digits in recording a data point in a log.

Lapses, on the other hand, appear to be a more covert form, apparently involving failures of memory. They may be revealed by an action taken as a consequence, but often they may only be realized by the person undergoing the lapse. Common forms of lapses include momentarily forgetting the name of the person with whom one is speaking on the telephone, or taking a familiar turn in the road (perhaps leading to the office) when the intention is to go to another, less familiar, destination. In a power plant, common forms of lapses would include mis-selecting components with similar identification labels, or remembering incorrectly a component number when being given verbal directions.

The incidence of slips and lapses appears, in both cases, to be influenced strongly by the levels of distractions and workload.

In practice, slips and lapses occur with a surprisingly high frequency. For example, anecdotal evidence indicates that pilots performing routine commercial flights may make up to about eight slips or lapses per hour. Yet rarely do these present a significant challenge to safety. First, the consequence of a slip or lapse is usually limited to one action associated with one or two pieces of equipment. Second, if indications are present to show that the intended action is not being achieved, and providing the consequence of the slip or lapse can be reversed, then recovery is common. Recovery often occurs because people are very resourceful in overcoming obstacles to a goal once problems are found to occur. For this reason, slips and lapses provide, in practice, only a modest contribution to risk as evaluated in PRAs.

Mistakes

Mistakes are unsafe acts arising from inadequate action planning rather than action execution. The planning may be "inadequate" because of misdiagnosis and therefore an inappropriate procedure is selected, or because of incorrect information contained in a procedure. These have been termed rule-based mistakes. The unsafe act may occur because procedures do not exist and the person performing the task has insufficient knowledge or incorrectly recalls information. These are knowledge-based mistakes.

In the review of experience at power plants, rule-based mistakes are one of the most frequent kinds of unsafe acts identified. In many cases, situations occur when a non-routine task is being performed, or a routine task is being performed during abnormal conditions and the procedures do not completely describe the required task. In

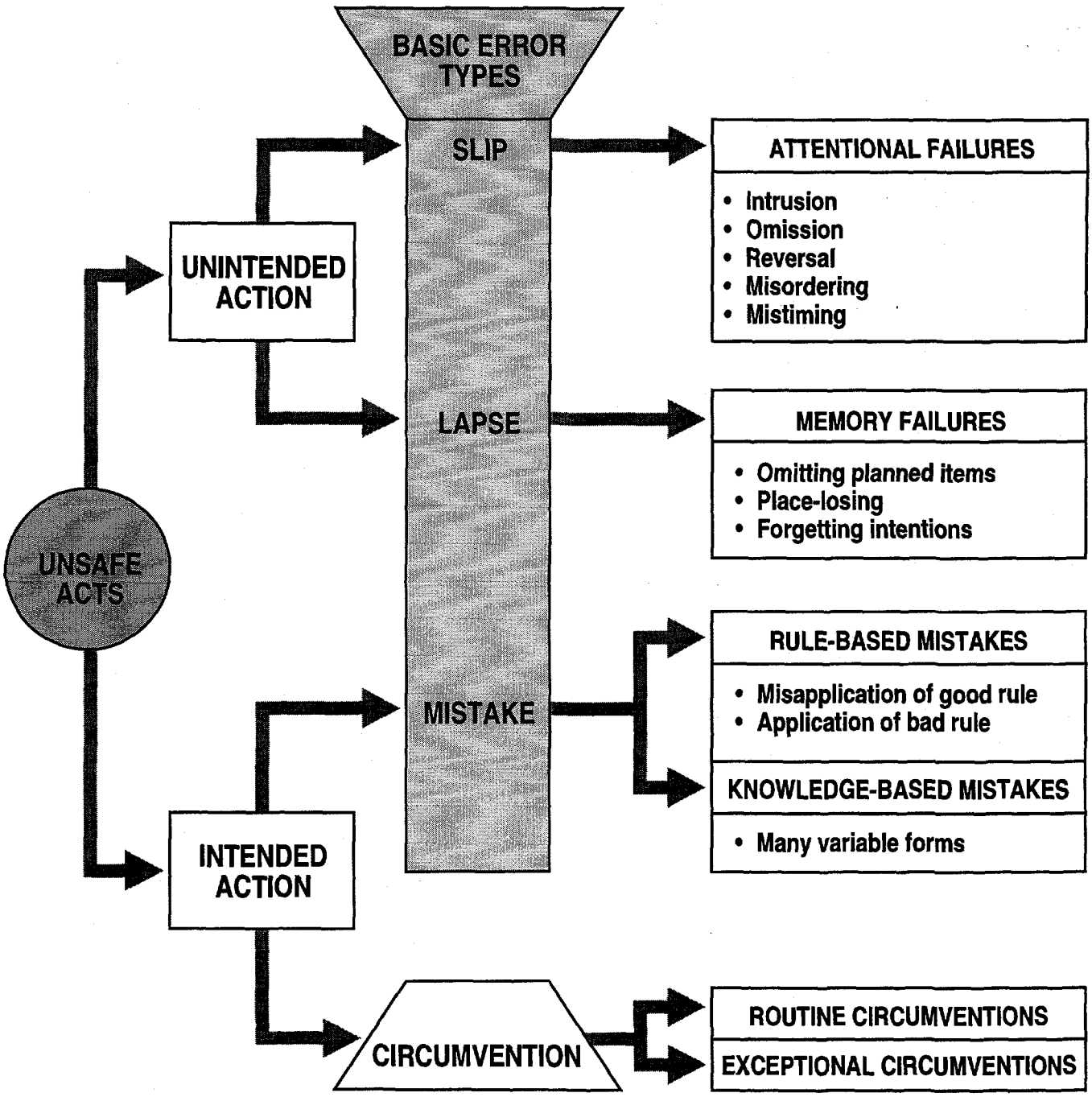
BASIC ERROR TYPES
SLIP
LAPSE
MISTAKE
UNSAFE ACTS
UNINTENDED ACTION
INTENDED ACTION
CIRCUMVENTION
ATTENTIONAL FAILURES
• Intrusion
• Omission
• Reversal
• Misordering
• Mistiming
MEMORY FAILURES
• Omitting planned items
• Place-losing
• Forgetting intentions
RULE-BASED MISTAKES
• Misapplication of good rule
• Application of bad rule
KNOWLEDGE-BASED MISTAKES
• Many variable forms
ROUTINE CIRCUMVENTIONS
EXCEPTIONAL CIRCUMVENTIONS

Figure E.1

consequence, the task is performed in a deficient manner. Such a situation arose in the response to the loss of all feedwater at Davis-Besse in 1985.[6]

Knowledge-based mistakes are most frequently encountered in power plant settings where some unusual combination of equipment and hardware failures occurs and operators have little or no procedural guidance to recover from the condition as they see it. The accident at Three Mile Island in 1979 was just such a case.[7] Since Three Mile Island, power plants have adopted the so-called symptom-based Emergency Operating Procedures (EOPs) in the belief that these procedures provide guidance for all conceivable accidents, and therefore knowledge-based mistakes may not be quite so important. However, as the NRC observed in its inspection program for emergency operating procedures, problems in the detailed implementation of the Owners' Groups EOP Guidelines have left some plants with major deficiencies in plant-specific EOPs.[8]

Mistakes may have multiple consequences in terms of the final actions performed. For example, if the incorrect procedure has been selected, then the plant personnel can purposefully follow several or all of the steps in that procedure. Those steps may lead the operators to place the plant in a worse state than by doing nothing. One scenario where this has been identified is the consequence of misdiagnosing a small-break loss-of-coolant accident (LOCA) in a pressurized water reactor (PWR) as a steam-generator tube rupture. In general, the strategy for a small-break LOCA is to maintain vessel inventory by increasing flow from the charging pumps; for a steam-generator tube rupture, it is to reduce vessel pressure, including the reduction of flow from the charging pumps. Hence the consequence of the mistake in diagnosis of a small-break LOCA as a steam-generator tube rupture would be to reduce the make-up flow, and thereby reduce the time to the onset of core damage compared with doing nothing.

The purposeful following of the incorrect procedure or knowledge-based strategy makes mistakes a much greater challenge to risk than the slips and lapses. In contrast to the (usually) simple recovery from a slip or lapse, operators are much less likely to realize that the strategy they are following is inappropriate. Once a strategy has been selected, people are remarkably reluctant to question its appropriateness and will pursue it even in the face of contradictory evidence. As a consequence, recovery from mistakes is less likely than from slips and lapses.

Circumventions

In contrast to slips, lapses, and mistakes, circumventions[9] are the deliberate breaking of safety rules and procedures, but with no intention of harm to the plant. For example, reversing two adjacent steps in a procedure may make the task much simpler and appear to the job performer to have no consequence in terms of plant safety. However, when some rare situation arises in which the sequencing of steps is important (as, for example, when other tasks are being performed concurrently), then this routine circumvention may lead to an accident.

Circumventions may occur for a variety of reasons. For many systems that have extensive webs of safety rules, procedures, and requirements, inconsistencies between these often exist such that the operator must compromise one rule to accomplish another. In other words, the system cannot be operated in accordance with all of the rules all of the time--the so-called system "double-bind". The accident at Chernobyl was perhaps the most dramatic consequence of a circumvention in that management pressure existed to complete the experiment even though the reactor power was outside the range specified for its performance ("power not to be less than 20%"). A second case is where operators, in their daily experience, learn that breaching some irritating rules appear to have no consequence in terms of safety and adopt work practices that breach the rules routinely. Rules written for rare plant conditions (such as power plant operators not sleeping in the control room) are the most likely to be challenged in this way.

The rate and significance of circumventions has not been the subject of extensive study in nuclear plant settings, but reviews of operational experience have not indicated that these unsafe acts have proved a major contribution to risk.

E.2.3 Selection of HRA Methods

The potential influences of the above error types on risk are summarized in Table E.1. No single HRA method applies to all types, and therefore the selection of a method or methods must be based on the kinds of errors expected to be important in the scenarios of interest in the PRA. Based on the above review, slips, lapses, and mistakes should be considered in the HRA study.

E.2.3.1 Slips and Lapses

Both slips and lapses are the principal focus of human reliability methods commonly used in NRC-sponsored PRAs, particularly the Technique for Human Error Rate Prediction (THERP)[10] and the Accident Sequence Evaluation Program (ASEP) methodology[11] used in the NRC's NUREG-1150 study. These evaluations require a task analysis to be performed of the task being analyzed to the level of individual actions (read procedural step, read meter, turn switch, etc.). For each action, important performance-shaping factors (PSFs) are identified and evaluated using the guidelines in the methodologies (location and labeling of switches, format of procedures, etc.). Based on these PSFs, failure probabilities are assigned for each action and then aggregated for the task as a whole. The potential for recovery from errors, such as a second operator checking the work of the first, are assessed using the methodologies guidelines.

This approach is considered appropriate by the HRA community for those failures that are not dynamic in nature (such as errors in maintenance and testing) where the pace or complexity of an emergency or abnormal condition is not a major factor.

E.2.3.2 Mistakes

For behavior in emergency or abnormal conditions, there are strong reservations[12] as to whether human reliability can be considered to be decompositional in the way THERP and similar methods imply. Such an approach neglects the overriding influences of errors in internal mental functions like cognition that are the cause of mistakes.

The human reliability assessment of mistakes has been considered in only the most rudimentary way, mostly focusing on the likelihood of misdiagnosis or erroneous strategy selection. Such errors have been estimated on the basis of time available (for thinking or for action). However, as discussed in Section 2.2.2, and in [12] and elsewhere, mistakes encompass more than simple errors in diagnosis. However, time still permits recovery from initial slips and lapses, and from rule-based mistakes. For example, time allows additional personnel to review the situation and check the initial actions; time allows the emergence of new information, and time allows the possibility of knowledge from training to override uncertainty in the validity of procedural steps. [However, it is recognized that the use of time as a basis for estimation of probabilities is an interim one pending the development of more comprehensive HRA methods.]

The most widely used methods for estimating the probability of mistakes use time/reliability correlations (T/RC), such as the operator action tree (OAT) method[13] or the THERP diagnosis screening method [see Reference 10]. [It is observed that the most frequently used T/RC, the HCR method[14]--

Table E.1 Potential Impact of Error Types on Risk

Unsafe Act	Frequency	Severity	Risk Impact
Slips & Lapses	High	Usually low	Low - moderate
Mistakes	Moderate - low	Moderate - high	Moderate - high
Circumventions	Low	Moderate - high	Low - moderate

specifically excludes errors in diagnosis or other mistakes (their so-called "P1 error") from its scope.] These T/RC methods provide an estimate of the probability that a correct diagnosis will be made and an appropriate strategy adopted, based on the time that operators have available for "thinking". Two other T/RC methods are also used for estimating probabilities with emphasis on mistakes; these are the method developed by Dougherty[15] and the method developed for recovery actions in the NRC's Risk Methods Integration and Evaluation Program (RMIEP).[16]

Any of these four methods can be used to estimate the likelihood of failure due to mistakes in the post-initiation phase. Of these four, the most economical to apply are the OAT and THERP nominal diagnosis models. [The THERP screening method (Table 12-2 of [10] is considered overly pessimistic for most cases, but the nominal model (Tables 12-4 and -5) is considered appropriate.]

It should be noted that research is continuing to develop improved models of mistake-driven human reliability. Such programs are mostly aimed at developing simulations of cognitive functions to identify the opportunities for, and consequences of, mistakes. However, no working HRA models using this approach are expected in the near future.

E.2.4 Representation of Errors in Systems Models

The failure modes associated with slips and lapses are often described in terms of "operator fails to close valve" or "operator fails to start pump", depending on the particular task. Such errors are rarely strongly conditional on the accident sequence provided the failure mode is relevant to the equipment. These errors can be incorporated and quantified in the system or functional fault trees.

However, the mistakes, being estimated on the basis of time available, are strongly influenced by the accident sequence conditions. Such errors should be evaluated in the event trees if possible, or at least at the highest levels of the fault trees where the probability can be adjusted according to the individual sequence timescales. In some cases, this may need to be done on a cutset-by-cutset basis if the timing information changes at that level.

The consequences of mistakes are usually expressed in terms of "operator fails to respond to event ...". These consequences should be considered as a common-mode failure to respond at all to the event. Recovery from mistakes, including the effects of multiple crew members, is implicit in the T/RC quantification

E.2.5 References

1. Dougherty, E., *HRA - Where Shouldst Thou Turn?*, In Reliability Engineering and System Safety, **29**, 1990, pp: 283-299

2. See, for example, the review of results of the exercise in Reason, J., *Human Error*, New York: Cambridge University Press, 1990, pp: 231-233.

3. Senders, J. W., and Moray, N. P., *Human Error, Cause, Prediction, and Reduction*, Hillsdale, NJ: Lawrence Erlbaum Associates, 1991.

4. See, for example, Meyer, O., *Interim Report: The Onsite Analysis of the Human Factors of Operational Events*, EGG-HFRU-9446, Idaho Falls, ID: Idaho National Engineering Laboratory, May 1991.

5. Wreathall, J., and Reason, J., *Human Errors and Disasters*, in Proceedings of the Fifth IEEE Conference on Human Factors and Power Plants, Monterey, CA, June 1992, New York: Institute of Electrical and Electronics Engineers, In Press.

6. US Nuclear Regulatory Commission, *Loss of Main and Auxiliary Feedwater Event at the Davis-Besse Plant on June 9, 1985*, NUREG-1154, Washington, D.C., 1985.

7. Kemeny, J., *The Need for Change: The Legacy of TMI*, Report of the President's Commission on the Accident at Three Mile Island, New York: Pergamon, 1979.

8. US Nuclear Regulatory Commission, *Lessons Learned From the Special Inspection Program for Emergency Operating Procedures*, NUREG-1358, Washington, D. C., April 1989.

9. The term used by the originator of the concept, James Reason, is "violations". However this term has other, specific, meanings in nuclear plant safety, and therefore the term "circumventions" has been adopted in the U.S. nuclear community.

10. Swain, A. D., and Guttmann, H. E., *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, Albuquerque, NM: Sandia National Laboratories, August 1983.

11. Swain, A. D., *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, NUREG/CR-4772, Albuquerque, NM: Sandia National Laboratories, February 1987.

12. See, for example, Hollnagel, E., *The Reliability of Man-Machine Interaction*, in Reliability Engineering and System Safety, 38, 1992, pp: 81-89.

13. Hall, R. E., Fragola, J. R., and Wreathall, J., *Post-Event Human Decision Errors: Operator Action Trees/Time Reliability Correlation*, NUREG/CR-3010, Upton, NY: Brookhaven National Laboratory, November 1983.

14. Hannaman, G. W., Spurgin, A. J., Lukic, Y. D., Human Cognitive Reliability Model for PRA Analysis, NUS-4531, Palo Alto, CA: Electric Power Research Institute, 1984.

15. Dougherty, E. M., and Fragola, J. R., *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*, New York: John Wiley & Sons, Inc., 1988.

16. Weston, L. M., Whitehead, D. W., and Graves, N. L., *Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP)*, NUREG/CR-4834, Albuquerque, NM: Sandia National Laboratories, June 1987.

E.3 Authors' Response

The reviewer states that our selection is based on Alan Swain's survey of HRA methods. We cited Swain's work only to show that there are additional ways of evaluating HRA methods. We felt that the RMIEP evaluations were well presented, and considered them as well as the Swain evaluations. However, our evaluations were done entirely independently, as should be evident from our narrative descriptions.

The reviewer also states that our evaluations lack currency. This may be true, as our evaluations were limited to work published between 1981 and 1987. We are not aware of any recent methods that offer advantages over the methods we evaluated, and that have been used widely enough to be recognized as useful.

In the paper, "Selection of HRA Methods," there is much emphasis on choice of terms. In Paragraph E.2.2.2, a "slip" is defined as "the inadvertent selection of the adjacent pump or valve control on a large control panel," whereas a "lapse" would include "mis-selecting components with similar identification labels". We do not feel that such fine nuances are of importance when conducting a real HRA.

He concludes that THERP and one of the time/reliability correlations (T/RC) methods would be his choices for our HRA. He prefers the OAT T/RC method, but acknowledges the utility of the Sandia Recovery Model.

The original text of Appendix D failed to clarify that a T/RC method would be used for diagnosis errors. As a result of the review, the text has been corrected. We agree that OAT is potentially useful, but we prefer the Sandia Recovery Model because it is based on more reliable data (from simulators).

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

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG/CR-6432
SEASF-DR-94-001

2. TITLE AND SUBTITLE

Estimated Net Value and Uncertainty for Automating ECCS Switchover at PWRs

3. DATE REPORT PUBLISHED

MONTH	YEAR
February	1996

4. FIN OR GRANT NUMBER

W6325

5. AUTHOR(S)

B. Walsh, J. Brideau, L. Comes, J. Darby, H. Guttmann, F. Sciacca, F. Souto, W. Thomas, G. Zigler

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Science and Engineering Associates, Inc.
6100 Uptown Blvd. NE
Albuquerque, NM 87110

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Commission and mailing address.)

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

10. SUPPLEMENTARY NOTES

J. Jackson, NRC Project Manager

11. ABSTRACT (200 words or less)

A central question for resolution of GSI-24 is whether or not PWRs that currently rely on a manual system for ECCS switchover to recirculation should be required to install an automatic system. Risk estimates are obtained by reevaluating the contributions to core damage frequencies (CDFs) associated with failures of manual and semiautomatic switchover at a representative PWR. This study considers each separate instruction of the corresponding emergency operating procedures (EOPs), the mechanism for each control, and the relationship of each control to its neighbors. Important contributions to CDF include human errors that result in completely coupled failure of both trains and failure to enter the required EOP. This detailed study finds that changeover to a semiautomatic system is not justified on the basis of cost-benefit analysis: going from a manual to a semiautomatic system reduces the CDF by 1.7x10-5 per reactor year, but the probability that the net cost associated with the modification being less than $1,000 per person-rem is about 20% without license renewal. Scoping analyses, using optimistic assumptions, were performed for a changeover to a semiautomatic system with automatic actuation and to a fully automatic system; in these cases the probability of having a net cost being less than $1,000/person-rem is about 50% without license renewal and over 95% with license renewal.

12. KEY WORDS/DESCRIPTORS (List word or phrases that will assist researchers in locating the report.)

ECCS Switchover
Human Reliability Resource
Generic Safety Issue 24

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

(This Page) Unclassified

(This Report) Unclassified

15. NUMBER OF PAGES

16. PRICE