NUREG/CR–4832
SAND92–0537
Vol. 5

Analysis of the LaSalle Unit 2 Nuclear Power Plant: Risk Methods Integration and Evaluation Program (RMIEP)

Parameter Estimation Analysis and Screening Human Reliability Analysis

Prepared by
T. A. Wheeler, A. D. Swain, J. A. Lambright, A. C. Payne, Jr.

Sandia National Laboratories
Operated by
Sandia Corporation

Prepared for
U.S. Nuclear Regulatory Commission

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

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

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

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

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

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

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

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

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

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

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

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

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, for use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

DISCLAIMER NOTICE

NUREG/CR–4832
SAND92–0537
Vol. 5
RX

Analysis of the LaSalle Unit 2 Nuclear Power Plant: Risk Methods Integration and Evaluation Program (RMIEP)

Parameter Estimation Analysis and Screening Human Reliability Analysis

Manuscript Completed: September 1992
Date Published: March 1993

Prepared by
T. A. Wheeler, A. D. Swain, J. A. Lambright, A. C. Payne, Jr.

Sandia National Laboratories
Albuquerque, NM 87185

Prepared for
Division of Safety Issue Resolution
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555
NRC FIN A1386

ABSTRACT

This volume describes the methodologies used in the data analysis, the screening human error analysis, and the common mode human error analysis performed in support of the LaSalle PRA. Selected results are presented in this volume. The remainder of the results are presented in other volumes of this report where they are actually used.

The data review process used in the determination of the data used for the initial screening analysis is described and the final screening data base is given. The IPRDS program was used to get more specific BWR-related data. This data was analyzed by Los Alamos National Laboratory using the FRAC code. The final data selection process is described and the final data distributions are presented. The actual implementation of the data base for the integrated accident sequence quantification is described in Volume 2 of this report on Integrated Quantification and Uncertainty Analysis.

Several new methods developed for use in analyzing both pre- and post-accident human errors for the initial screening analysis are described. Most of the actual results are given in other volumes of this report under the appropriate sub-analysis descriptions. A method for determining procedural common mode analysis is described and the results presented.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Concluded)

LIST OF FIGURES

LIST OF TABLES

LIST OF TABLES (Concluded)

FOREWORD

LaSalle Unit 2 Level III Probabilistic Risk Assessment

In recent years, applications of Probabilistic Risk Assessment (PRA) to nuclear power plants have experienced increasing acceptance and use, particularly in addressing regulatory issues. Although progress on the PRA front has been impressive, the usage of PRA methods and insights to address increasingly broader regulatory issues has resulted in the need for continued improvement in and expansion of PRA methods to support the needs of the Nuclear Regulatory Commission (NRC).

Before any new PRA methods can be considered suitable for routine use in the regulatory arena, they need to be integrated into the overall framework of a PRA, appropriate interfaces defined, and the utility of the methods evaluated. The LaSalle Unit 2 Level III PRA, described in this and associated reports, integrates new methods and new applications of previous methods into a PRA framework that provides for this integration and evaluation. It helps lay the bases for both the routine use of the methods and the preparation of procedures that will provide guidance for future PRAs used in addressing regulatory issues. These new methods, once integrated into the framework of a PRA and evaluated, lead to a more complete PRA analysis, a better understanding of the uncertainties in PRA results, and broader insights into the importance of plant design and operational characteristics to public risk.

In order to satisfy the needs described above, the LaSalle Unit 2, Level III PRA addresses the following broad objectives:

1. To develop and apply methods to integrate internal, external, and dependent failure risk methods to achieve greater efficiency, consistency, and completeness in the conduct of risk assessments;

2. To evaluate PRA technology developments and formulate improved PRA procedures;

3. To identify, evaluate, and effectively display the uncertainties in PRA risk predictions that stem from limitations in plant modeling, PRA methods, data, or physical processes that occur during the evolution of a severe accident;

4. To conduct a PRA on a BWR 5, Mark II nuclear power plant, ascertain the plant's dominant accident sequences, evaluate the core and containment response to accidents, calculate the consequences of the accidents, and assess overall risk; and finally

5. To formulate the results in such a manner as to allow the PRA to be easily updated and to allow testing of future improvements in methodology, data, and the treatment of phenomena.

The LaSalle Unit 2 PRA was performed for the NRC by Sandia National Laboratories (SNL) with substantial help from Commonwealth Edison (CECo) and its contractors. Because of the size and scope of the PRA, various related programs were set up to conduct different aspects of the analysis. Additionally, existing programs had tasks added to perform some analyses for the LaSalle PRA. The responsibility for overall direction of the PRA was assigned to the Risk Methods Integration and Evaluation Program (RMIEP). RMIEP was specifically responsible for all aspects of the Level I analysis (i.e., the core damage analysis). The Phenomenology and Risk Uncertainty Evaluation Program (PRUEP) was responsible for the Level II/III analysis (i.e., accident progression, source term, consequence analyses, and risk integration). Other programs provided support in various areas or performed some of the subanalyses. These programs include the Seismic Safety Margins Research Program (SSMRP) at Lawrence Livermore National Laboratory (LLNL), which performed the seismic analysis; the Integrated Dependent Failure Analysis Program, which developed methods and analyzed data for dependent failure modeling; the MELCOR Program, which modified the MELCOR code in response to the PRA's modeling needs; the Fire Research Program, which performed the fire analysis; the PRA Methods Development Program, which developed some of the new methods used in the PRA; and the Data Programs, which provided new and updated data for BWR plants similar to LaSalle. CECo provided plant design and operational information and reviewed many of the analysis results.

The LaSalle PRA was begun before the NUREG-1150 analysis and the LaSalle program has supplied the NUREG-1150 program with simplified location analysis methods for integrated analysis of external events, insights on possible subtle interactions that come from the very detailed system models used in the LaSalle PRA, core vulnerable sequence resolution methods, methods for handling and propagating statistical uncertainties in an integrated way through the entire analysis, and BWR thermal-hydraulic models which were adapted for the Peach Bottom and Grand Gulf analyses.

The Level I results of the LaSalle Unit 2 PRA are presented in: "Analysis of the LaSalle Unit 2 Nuclear Power Plant: Risk Methods Integration and Evaluation Program (RMIEP)," NUREG/CR-4832, SAND92-0537, ten volumes. The reports are organized as follows:

NUREG/CR-4832 - Volume 1: Summary Report.

NUREG/CR-4832 - Volume 2: Integrated Quantification and Uncertainty Analysis.

NUREG/CR-4832 - Volume 3: Internal Events Accident Sequence Quantification.

NUREG/CR-4832 - Volume 4: Initiating Events and Accident Sequence Delineation.

NUREG/CR-4832 - Volume 5: Parameter Estimation Analysis and Human Reliability Screening Analysis.

NUREG/CR-4832 - Volume 6: System Descriptions and Fault Tree Definition.

NUREG/CR-4832 - Volume 7: External Event Scoping Quantification.

NUREG/CR-4832 - Volume 8: Seismic Analysis.

NUREG/CR-4832 - Volume 9: Internal Fire Analysis.

NUREG/CR-4832 - Volume 10: Internal Flood Analysis.

The Level II/III results of the LaSalle Unit 2 PRA are presented in: "Integrated Risk Assessment For the LaSalle Unit 2 Nuclear Power Plant: Phenomenology and Risk Uncertainty Evaluation Program (PRUEP)," NUREG/CR-5305, SAND90-2765, 3 volumes. The reports are organized as follows:

NUREG/CR-5305 - Volume 1: Main Report

NUREG/CR-5305 - Volume 2: Appendices A-G

NUREG/CR-5305 - Volume 3: MELCOR Code Calculations

Important associated reports have been issued by the RMIEP Methods Development Program in: NUREG/CR-4834, Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP); NUREG/CR-4835, Comparison and Application of Quantitative Human Reliability Analysis Methods for the Risk Methods Integration and Evaluation Program (RMIEP); NUREG/CR-4836, Approaches to Uncertainty Analysis in Probabilistic Risk Assessment; NUREG/CR-4838, Microcomputer Applications and Modifications to the Modular Fault Trees; and NUREG/CR-4840, Procedures for the External Event Core Damage Frequency Analysis for NUREG-1150.

Some of the computer codes, expert judgement elicitations, and other supporting information used in this analysis are documented in associated reports, including: NUREG/CR-4586, User's Guide for a Personal-Computer-Based Nuclear Power Plant Fire Data Base; NUREG/CR-4598, A User's Guide for the Top Event Matrix Analysis Code (TEMAC); NUREG/CR-5032, Modeling Time to Recovery and Initiating Event Frequency for Loss of Off-Site Power Incidents at Nuclear Power Plants; NUREG/CR-5088, Fire Risk Scoping Study: Investigation of Nuclear Power Plant Fire Risk, Including Previously Unaddressed Issues; NUREG/CR-5174, A Reference Manual for the Event Progression Analysis Code (EVNTRE); NUREG/CR-5253, PARTITION: A Program for Defining the Source Term/Consequence Analysis Interface in the NUREG-1150 Probabilistic Risk Assessments, User's Guide; NUREG/CR-5262, PRAMIS: Probabilistic Risk Assessment Model Integration System, User's Guide; NUREG/CR-5331, MELCOR Analysis for Accident Progression Issues; NUREG/CR-5346, Assessment of the XSOR Codes; and NUREG/CR-5380, A

User's Manual for the Postprocessing Program PSTEVNT. In addition the reader is directed to the NUREG-1150 technical support reports in NUREG/CR-4550 and 4551.

Arthur C. Payne, Jr.
Principal Investigator
Phenomenology and Risk Uncertainty Evaluation Program and
Risk Methods Integration and Evaluation Program
Division 6412, Reactor Systems Safety Analysis
Sandia National Laboratories
Albuquerque, New Mexico 87185

1.0 INTRODUCTION

This report describes the methodology used in certain subanalyses of the LaSalle PRA and presents selected results. The subanalysis areas are: the screening and final data analysis, the screening human factors analysis, and the procedural common cause analysis.

The data analysis for the LaSalle PRA was extensive and extended over several years. This volume contains a description of how point-estimates were obtained for the screening analysis, how the data was further analyzed for the final accident sequence quantification, and the final mean values and uncertainty distributions selected. This is limited to mechanical failures of components and human errors. The failure of components due to severe environments produced in the reactor building after containment venting or structural failure is described in Volume 3 of this report.

The analysis of human errors for the LaSalle PRA was very comprehensive. First, to identify pre-accident errors, all the LaSalle procedures (test, maintenance, and operating) were reviewed by the system analysts to determine if the procedures affected any system components and then the analysts identified any steps in the procedures where failure of the operator to correctly perform the step could affect system or component performance (the procedure used is described in Volume 6 of this report on the systems analysis). Many test and maintenance errors were identified at this stage.

Second, screening rules were developed to identify which of these errors were significant enough to be included on the fault trees. The screening rules developed for this step are described in Chapter 3 of this volume. Even after application of the screening rules many human errors remained and they were included in the fault trees by the system analysts.

Third, in order to identify human errors that might have been missed by examining individual systems only, a global analysis was performed. The LaSalle procedures were explicitly examined to identify specific procedures and procedural steps that had the potential to affect more than one system. The procedure used and the results of this analysis are described in Chapter 4 of this volume.

Fourth, since the post-accident operator actions (usually called operator recovery actions) depend very strongly on the specific timing of the accident sequence, which is represented by the specific individual component failures that makeup the accident sequence cut sets; very little credit is given for these kinds of actions in the screening analysis and very few of them are placed directly on the fault trees. Only a limited number of operator actions prescribed by procedure are included in the initial model, usually only those actions having to do with the manual operation of manually operated systems (i.e., systems which have no automatic actuation but must always be turned on by the operator). As described in Chapter 3 of this volume some screening rules were also developed for quantification of these events.

Fifth, after the accident sequence cut sets were obtained, each cut set was individually examined and possible operator actions to recover from the failures in the cut set were determined. The time in which the operator action could be successful was determined for the different component failure combinations using both accident sequence thermal/hydraulic code results and system component response information from the LaSalle utility Commonwealth Edison Company (CECo) and the architect/engineer Sargent & Lundy (S&L). The results of this analysis are described in Volume 3 of this report.

Sixth, a completely new method was developed, based on the use of the LaSalle simulator, to classify and quantify these operator recovery actions as described in References 1 and 2. Finally, the appropriate actions were selected and events representing them were added to the cut sets for the final analysis. This process is described in Volume 3 of this report.

1.1 References

1. L. M. Weston, D. W. Whitehead, and N. L. Graves, "Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP), Volume 1: Data Based Method," NUREG/CR-4834/1 of 2, SAND87-0179, Sandia National Laboratories, Albuquerque, NM, June 1987.

2. D. W. Whitehead, "Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP), Volume 2: Application of the Data Based Method," NUREG/CR-4834/2 of 2, SAND87-0179, Sandia National Laboratories, Albuquerque, NM, December 1987.

2.0 PARAMETER ESTIMATION ANALYSIS

2.1 Introduction

The task described in this chapter is that of estimating event probabilities and failure rates. These estimates are used to evaluate the probabilities of occurrence of the basic events appearing in the system fault trees. The estimation of initiating event frequencies also falls into this task. Probabilities and failure rates used in quantifying basic events must be evaluated for all the plant components included in the system models and for the various failure modes of each component. For example, circuit breakers represent one type of component modeled in the LaSalle PRA. A circuit breaker can fail in several different modes. Some are demand related failures - Fail-to-Open, or Fail-to-Close on demand. Other failure modes represent failure to complete a mission over a period of time - Fail-to-Remain-Open, or Fail-to-Remain-Closed over a specified time interval.

A point estimate PRA generated by using mean values of the data, appropriately correlated if necessary, represents the mean state of the plant over the life of the plant (in some cases, the data may be used to evaluate the state of the plant at a particular time; but, for general risk evaluation we are trying to estimate the risk at any time during the plant life). A particular PRA model may change both in its structure (due to mechanical changes in the plant design over time) and in the data used to quantify the model. PRAs do not usually try to account for future design changes. In any case, the model may be modified to evaluate the effect of any specific design change before or after the change is made. The PRA, therefore, should roughly represent the underlying reliability of the plant given that the design remains constant over the life of the plant (since if the design changes this can be reevaluated at that time). However, there is uncertainty as to what is the appropriate set of failure probabilities for the components making up the plant model.

The uncertainty in the failure probabilities enters from various sources. First, the data used to calculate the failure probabilities is, in many cases, limited. Second, the accident sequences used in the PRA are defined only in the most general way (i.e., accident occurs at power and a specific set of systems fail). Partial component failures, specific initial conditions such as the reactor power at the time of the incident, the time during the refueling cycle, environmental conditions, etc. are not evaluated. These can affect the event quantification in various ways. An accident sequence will occur at a specific time; however, the PRA models it as occurring at any time. Therefore, the effect of varying the power level, the primary water level, the time during the refueling cycle, and the power history all must be taken into account in the evaluation of the accident sequence timing and the effectiveness of the operator response. The specific weather conditions at the time of the accident (summer or winter for example) and environmental history may have an effect on the component reliabilities or simply make them more susceptible to specific

accident conditions such as severe environments produced in the reactor building after containment failure or venting. The effectiveness of the operators will vary from crew to crew and with the emotional state of the people themselves on a daily basis. This induces additional uncertainty into the quantification of the operator response.

In addition to all of the above, the degree of confidence that is associated with these parameter estimates can vary depending on the amount of data available, how well defined the component boundary is, how applicable the data is to that component, or how well a particular failure mode is understood. For failure rates and probabilities which represent unusual events, very little data is available for a specific plant and components must be grouped with similar components from other plants to generate a data base large enough to have any hope of getting reasonable estimates of the parameter values. The lack of a well coordinated and consistent data base makes the evaluation and interpretation of the final estimates somewhat difficult.

We attempt to capture most of the above uncertainty in the PRA by defining probability distributions for each parameter which specify the range of values which the parameter can have. This uncertainty is incorporated into the probabilities of the basic events of the system models and propagated through the accident sequence analysis to yield a probabilistic uncertainty characterization of the Probabilistic Risk Assessment (PRA) output - whether it be core damage frequency or risk.

The RMIEP parameter estimation task encountered several difficulties in deriving event estimates and uncertainties for LaSalle. Ideally, a plant specific analysis such as RMIEP would utilize plant specific data for parameter estimation; however, PRA studies model unusual events. An individual plant can hardly supply sufficient data to model all component failure modes accurately. Plant specific data should be used when available in a useful format, but PRA has had to rely extensively on generic parameter estimates. Generic estimates are based on the experience at all nuclear power plants; therefore, the pool of knowledge regarding an individual component failure is enlarged. At the time of this analysis (1988), the LaSalle plant had limited plant specific data due to its newness, so the use of generic data in RMIEP was necessary, but the generic parameter estimates present problems as well. LaSalle has several new component designs which are not accounted for in the experience of the nuclear industry.

RMIEP represents the most detailed PRA performed to date in terms of its system models. As the sophistication and detail of PRA models increase, inadequacies in data collection and parameter estimation become greater. Data on components and failure modes not previously modeled are often unavailable or poorly analyzed. Furthermore, accurate parameter estimation is difficult without good records of such items as the number of times components have been demanded or the amount of time - either standby or operational - that components have existed in a certain state. The quality

and quantity of data collection and analysis is not commensurate with the current needs of PRA models.

The limitations of data and data analyses with respect to parameter estimation does not discount the value of PRA as a tool to guide both plant operators and regulators. RMIEP adheres to a policy of conservatisms when difficulties in parameter estimation occur. It is important that potential accident sequences not "fall through the cracks" of the analysis.

The following sections detail how the RMIEP parameter estimation task moves from an initially simplistic, conservative screening analysis to a more comprehensive analysis which incorporates estimation uncertainty and engineering insights to achieve a reasonable and informative representation of the performance of components for LaSalle.

Section 2.2 discusses the process by which a set of events and their failure modes were developed from the systems analysis of LaSalle, and how parameter estimates for the failure rates and/or probabilities were assigned to these events and failure modes for the initial screening quantification of the system and accident models. Section 2.3 discusses how component failure rates and probabilities are incorporated into the basic events of the fault trees and accident sequence equations. Section 2.4 discusses the refinement of the screening parameter estimates presented in Section 2.2 from a set of conservative, point estimate values to a best case set of values with uncertainty models based on data analyses. Section 2.5 discusses the method used to model the probabilistic uncertainty of parameter estimates and basic events. Section 2.6 presents the results of the final RMIEP parameter estimate analyses used in the LaSalle PRA.

2.2 Parameter Estimates for Screening Analysis

2.2.1 Introduction

The process of analyzing large, detailed system fault trees in the context of event tree accident sequences can generate very large and unmanageable numbers of cut sets. It is necessary to reduce the size of accident sequence models for logistical purposes - both for the analyst and because of computer limitations. This is achieved by screening out the non-dominant portions of the system and accident models as the development of accident models proceeds from the system fault tree solution to the merging of system fault trees for accident sequences to the solving of the accident models. At each step of the process, combinations of basic events whose values fall below specified threshold levels are deleted to streamline the analysis. Conservatism is vital in the screening process for modeling those events which have variable failure rates depending on the accident conditions or those events for which insufficient data is available for assigning accurate probabilities. It is much easier to lower certain event values at later stages of the analysis than to significantly increase them after many event combinations have been deleted. Then, one would have to

retrace fault tree and accident sequence solution steps to pick up formerly non-dominant events which now may become dominant. Later sections will discuss in more detail the process of quantifying and screening of system fault trees and accident sequences.

In this section, the process of compiling a set of screening parameter estimates which were used in the initial basic event quantification is described. The values used for failure mode screening quantification are presented here as well. These values are the result of the initial screening quantification and should not be construed as the estimates used in the RMIEP models. The final parameter estimates are presented in Section 2.6.

2.2.2 Parameter Estimation Method

The process of analyzing systems and constructing system models produces the set of components and failure modes, maintenance actions, and tests which are used to construct the basic events of the system models. The systems analysis for LaSalle generated a set of 284 component failure modes. This set is shown in Tables 2.1 through 2.5 and includes all the various test, maintenance, component faults, and initiating events which contributed to the events of the system fault trees and accident sequence models. Human actions are described in Chapter 3 of this volume.

The numerical values assigned to the items of Tables 2.1 through 2.5 represent the results of reviewing many of the reports and data analyses of the references. Wherever possible, values were taken from this set of "generic" parameter estimation analyses and assigned to the appropriate failure modes. The survey of the reports was used to select a point estimate for each failure mode. The point estimate represents a middle ground of published values. Some component failure modes or events represent black box type events, such as the Gland Sealing System in Table 2.1. Events such as these are not analyzed in data analyses. Some were assigned values of 1.0 to ensure that, if they were thought to be potentially significant, they would pass through the screening analysis and be analyzed in depth at a later phase. Other black box events were quantified by referring to other PRAs that modeled similar events. In such cases, conservative estimates based on other PRAs were used for screening. Despite such conservative treatment of black box events, many of these events were still deleted by the system fault tree screening quantification, at a great savings of analyst effort and resources.

In general, using the mean value from the observed failure values will give a reasonable estimate of the failure probability of a component. However, this assumes that the components represent, in some sense, a homogeneous group with similar physical and operating characteristics. In some cases, specific components are tested at much longer intervals than the bulk of the components which make up the data base.

Table 2.1
Failure Mode Screening Estimates

Component	Failure Mode[a]	Event Code[a]		Best Estimate	Source
Motor-Driven Pump	FTS	FTS	(1)	3.0E-3	IREP,LER
	FTR	FTR	(2)	3.0-5/hr.	IREP
Standby Liq. Cont. Pump	FTS		(22)	1.0E-2	IPRDS
Turbine-Driven Pump	FTS	FTS	(3)	3.0E-2	IREP,LER
	FTR	FTR	(4)	1.0E-4/hr.	NREP,IPRDS
Air-Op. Valve	FTO FTC	FTOP	(5)	1.0E-3	LER
	FTRO		(6)	1.0E-7/hr.	IPRDS,ASEP IREP
	FTRC		(7)	3.0E-7/hr.	IPRDS, LER
Check Valve	FTO	FTO	(8)	1.0E-4	IREP,LER
	FTC		(9)	1.0E-3	IREP
	FTRO		(6)	1.0E-7/hr.	IPRDS,IREP
	FTRC		(7)	3.0E-7/hr.	IPRDS,IREP
Manual-Op. Valve	FTO FTC	FTOP	(12)	1.0E-4	IREP,LER
	FTRO		(6)	1.0E-7/hr.	IPRDS
	FTRC		(7)	3.0E-7/hr.	IPRDS

Table 2.1
Failure Mode Screening Estimates (Continued)

Component	Failure Mode[a]	Event Code[a]	Best Estimate	Source
Motor-Op. Valve	FTO FTC	FTOP (13)	3.0E-3	LER,IREP
	FTRO	(6)	1.0E-7/hr.	LER
	FTRC	(7)	3.0E-7/hr.	IREP
Safety Rel. Valve	FTO (relief mode)	(14)	1.0E-5	IREP
	FTO (ADS mode)	(15)	1.0E-3	IREP
	Premature Open	(16)	3.0E-6/hr.	LER
	FTC	(17)	3.0E-2	IREP
Solenoid Valve	FTO FTC	FTOP (18)	1.0E-3	IREP
Hydraulic Valve	FTO FTC	FTOP (19)	1.0E-3	IREP,IPRDS
Explosive Valve	FTOP	(20)	neg.	
Battery	FTDP	(26)	1.0E-6/hr.	IEEE
Battery Charger	FTDP	(27)	1.0E-6/hr.	IREP
Bus	Open circuit	Open (28)	1.0E-7/hr.	IEEE
Circuit Breaker	FTO FTC	FTOP (29)	3.0E-3	IREP

Table 2.1
Failure Mode Screening Estimates (Continued)

Component	Failure Mode[a]	Event Code[a]	Best Estimate	Source
Circuit Breaker (Continued)	Spurious Transfer	SOP (30)	3.0E-5/hr.	IREP
Diesel Generators	FTS	FTS (31)	3.0E-2	IREP
	FTR	FTR (32)	3.0E-3/hr.	IREP
Time Delay Relay	Spurious Transfer	SOP (33)	3.0E-4	IREP
Coil	FT Energize	(37)	3.0E-6/hr.	IREP
	FT Remain Energized	(38)	3.0E-6/hr.	IREP
Contact Pair	FTO FTC	FTOP (39)	3.0E-4	IREP
	Spurious Open	(40)	1.0E-7/hr.	WASH-1400
	Spurious Close	(41)	3.0E-8/hr.	WASH-1400
Inverter	FTOP	(35)	1.0E-4/hr.	IREP
Transformer	FTDP	(36)	1.0E-6/hr.	IREP
Condensate Demin.	Rupture	(51)	3.0E-6/hr.	See Event Code 58
	Blockage	(52)	3.0E-5/hr	See Event Code 57
Damper	FTOP	FTOP (53)	3.0E-3	IREP
	FTRO	(54)	1.0E-7/hr.	

Table 2.1
Failure Mode Screening Estimates (Continued)

Component	Failure Mode[a]	Event Code[a]	Best Estimate	Source
Filter, Air	Failure	(55)	1.0E-5/hr.	NPRDS
Filter, Water	Blockage	(56)	3.0E-5/hr.	IREP
Heat Exchanger	Blockage	(57)	3.0E-6/hr.	EG&G CRBRP
	Rupture	(58)	3.0E-6/hr.	IREP
L. P. Heater	Blockage	(59)	3.0E-6/hr.	IEEE
	Rupture	(60)	3.0E-6/hr.	See Event 58
Main Condenser	Rupture	(61)	3.0E-6/hr.	See Event 58
	Blockage	(62)	3.0E-6/hr.	See Event 57
Off-Gas Cond.	Rupture	(63)	3.0E-6/hr.	See Event 58
	Blockage	(64)	3.0E-6/hr.	See Event 57
Pump Oil Cooler	Rupture	(65)	3.0E-6/hr.	See Event 58
	Blockage	(66)	3.0E-6/hr.	See Event 57
Spool Piece	Leakage	(67)	1.0E-10/hr.	See Event 122
St. Jet Air Ejector	Rupture	(68)	1.0E-10/hr.	See Event 122
	Blockage	(69)	1.0E-10/hr.	See Event 123
St. Packing Exhauster	Rupture	(70)	3.0E-6/hr.	See Event 58
	Blockage	(71)	3.0E-6/hr.	See Event 57
Strainer	Blockage	(72)	3.0E-5/hr.	IREP

Table 2.1
Failure Mode Screening Estimates (Continued)

Component	Failure Mode[a]	Event Code[a]	Best Estimate	Source
Vane Axial Fan	FTS	(73)	3.0E-4	WASH-1400
	FTR	(74)	1.0E-5/hr.	WASH-1400
Vent Supply Filter	Blockage	(75)	1.0E-5/hr.	NPRDS-air filter
Stm. Line Cond. Trap	Open	(76)	1.0E-10/hr.	See Event 122
Rupture Disk	FTRC	(77)	3.0E-6/hr.	NPRDS
Steam Condenser	Leak	(78)	3.0E-6/hr.	See Event 58
Cooler	Rupture	(79)	3.0E-5/hr.	EG&G-CRBRP (Chiller)
	Blockage	(80)	3.0E-6/hr.	See Event 57
Elec. Heater	FTR	(81)	3.0E-6/hr.	IEEE
Pipe Heater	FTR	(82)	1.0E-6/hr.	IEEE
Expansion Tank	Rupture	(84)	3.0E-6/hr.	See Event 58
Diesel-Driven Pump	FTS	(85)	3.0E-3	IREP,IPRDS
	FTR	(86)	1.0E-3/hr.	IREP
Vacuum Breakers	FTO	(87)	1.0E-5	IREP
	FTC	(88)	1.0E-5	IREP
Relief Valves (non-safety)	FTO	(89)	3.0E-4	IREP
	FTR	(90)	3.0E-2	IREP

Table 2.1
Failure Mode Screening Estimates (Continued)

Component	Failure Mode[a]	Event Code[a]	Best Estimate	Source
Stop Check Valves	FTO	(91)	1.0E-4	IREP
Switches - Torque	FTOP	(92)	1.0E-4	IREP
Switches - Limit	FTOP	(93)	1.0E-4	IREP
Switches - Pressure	FTOP	(94)	1.0E-4	IREP
Switches - Manual	FTT	(95)	3.0E-5	IREP
Fuses	Prem. Open	(96)	3.0E-6/hr.	IREP
Orifices	Blockage	(97)	3.0E-4	IREP
	Rupture	(98)	3.0E-8/hr.	IREP
DC Motor-Generators	FTOP	(99)	3.0E-6/hr.	IREP
Wires (per unit)	Open	(100)	3.0E-6/hr.	IREP
	Short	(101)	3.0E-7/hr.	IREP
Solid State Devices	Failure	(102)	3.0E-6/hr.	IREP
Terminal Boards	Open	(103)	3.0E-7/hr.	IREP
	Short	(104)	3.0E-7/hr.	IREP
Air Coolers	FTOP	(105)	1.0E-5/hr.	IREP

Table 2.1
Failure Mode Screening Estimates (Continued)

Component	Failure Mode[a]	Event Code[a]	Best Estimate	Source
Instrumentation:				
Level Sensor	Sensing Line/ Rupture	(111)	1.0E-8/hr.	WASH-1400
	Sensing Line/ Blockage	(112)	1.0E-8/hr.	WASH-1400
	Element	(113)	3.0E-6/hr.	IREP,IEEE,LER
Pressure Sensor	Sensing Line/ Rupture	(111)	1.0E-8/hr.	WASH-1400
	Sensing Line/ Blockage	(112)	1.0E-8/hr.	WASH-1400
	Element	(113)	3.0E-6/hr.	IREP,IEEE,LER
Temperature	Element	(113)	3.0E-6/hr.	IREP,IEEE,LER
Solenoid Valve	FTRO	(6)	1.0E-7/hr.	Same as AOV
Solenoid Valve	FTRC	(7)	3.0E-7/hr.	Same as AOV

Table 2.1
Failure Mode Screening Estimates (Continued)

Component	Failure Mode[a]	Event Code[a]	Best Estimate	Source
MSIV Valve	FTRO	(6)	1.0E-7/hr.	Same as AOV
MSIV Valve	FTRC	(7)	3.0E-7/hr.	Same as AOV
Pressure Reg.	FTREG	(129)	7.0E-5/hr.	NPRDS
Relief Valves (NS)	REM OPEN	(124)	3.0E-6/hr.	See Event Code 16
Pipe	Blockage (Due to Boron)	(125)	1.0E-9/hr.	10 X Event Code 123
Pipe	Rupture (Per Section)	(122)	1.0E-10/hr.	WASH-1400
Pipe	Blockage (Per Section)	(123)	1.0E-10/hr.	WASH-1400
Shaft Speed Changes	Premature if Disengaged	(127)	1.0E-6/hr.	WASH-1400 (Clutch)
Air Dryers	Blockage	(130)	3.0E-5/hr.	Similar to Event Code 72
Auto Flush Strainer	Blockage	(135)	3.0E-5/hr.	Similar to Event Code 72
SP Suction Strainer	FTC	FTOP (143)	1.0E-3	Similar to Event Code 72

Table 2.1
Failure Mode Screening Estimates (Continued)

Component	Failure Mode[a]	Event Code[a]	Best Estimate	Source
Damper Cont. Cir.	FTC	(142)	1.0E-3	Similar to Event Code 114
Duct	Rupture	(141)	1.0E-10/hr.	Similar to Event Code 72
DV Relay	Spur Deenergize	(136)	4.0E-6/hr.	2 UV Relays + Relay Coil
DV Relay	FT Deenergize	(137)	1.0E-8/hr.	See Event Code 133
UV Relay	Spur Deenergize	(138)	6.0E-7/hr.	NPRDS
Relay Coil	FT Deenergize	(133)	1.0E-8/hr.	WASH-1400
Diesel Gen. Cont. Circuit	FTS	(139)	1.0E-3	30% of Event Code 31
Diesel Gen. Cont. Circuit	FTR	(140)	1.0E-3/hr.	30% of Event Code 32
Strainer (Timer)	FTCYCLE	(134)	3.0E-5/hr.	Similar to Event Code 72
SOV Cont. Circuit	FTO	FTOP (116)	1.0E-4	See AOV Control Circuit
SOV Cont. Circuit	FTRO	SOP (118)	3.0E-6/hr.	See AOV Control Circuit
CST	Blockage	(144)	3.0E-6/hr.	Similar to HTX (57)
CST	Rupture	(128)	3.0E-6/hr.	Similar to HTX (58)

Table 2.1
Failure Mode Screening Estimates (Continued)

Component	Failure Mode[a]	Event Code[a]	Best Estimate	Source
Expansion Tank	Blockage	(145)	3.0E-6/hr.	Similar to HTX (57)
Pressurized Tank	Blockage	(146)	3.0E-6/hr.	Similar to HTX (57)
Pressurized Tank	Rupture (Leak)	(126)	3.0E-6/hr.	Similar to HTX (58)
Nitrogen Bottles	Blockage	(131)	3.0E-6/hr.	Similar to HTX (57)
Nitrogen Bottles	Rupture (Leak)	(132)	3.0E-6/hr.	Similar to HTX (58)
Compressor Positive	FTOP	(119)	1.0E-5/hr.	WASH-1400 See Event 74
Compressor Centrif.	FTOP	(120)	1.0E-6/hr.	Assumed 1/10 * (119)
Compressor AXAGL	FTOP	(121)	1.0E-7/hr.	Assumed 1/100 * (119)
MOV Control Circuit	FTO	FTOP (114)	1.0E-3	LER
MOV Control Circuit	FTRO	SOP (117)	6.0E-7/hr.	2 Wires + 1 Contact Pair
Fan Control Circuit	FTS	(114)	1.0E-3	Similar MOV Cont. Circuit
Circuit Breaker Control Circuit	FTO FTC	FTOP (114)	1.0E-3	Similar MOV Cont. Circuit
Circuit Breaker Control Circuit	FTRO	SOP (117)	6.0E-7/hr.	Similar MOV Cont. Circuit

Table 2.1
Failure Mode Screening Estimates (Continued)

Component	Failure Mode[a]	Event Code[a]	Best Estimate	Source
Motor Pump Control Circuit	FTS	(114)	1.0E-3	Similar MOV Cont. Circuit
Motor Pump Control Circuit	FTR	(117)	6.0E-7/hr.	Similar MOV Cont. Circuit
Turbine Pump Control Circuit	FTS	(115)	3.0E-3	LERs
Turbine Pump Control Circuit	FTR	(143)	3.0E-5/hr.	30% of Event Code 4
AOV Control Circuit	FTO	FTOP (116)	1.0E-4	1 Relay Coil Tested Monthly
AOV Control Circuit	FTRO	SOP (118)	3.0E-6/hr.	1 Coil, FTR Energized

Table 2.1
Failure Mode Screening Estimates (Concluded)

a. abbreviations:

FTS	Fail-to-Start
FTR	Fail-to-Run
FTO	Fail-to-Open
FTC	Fail-to-Close
FTRO	Fail-to-Remain-Open (plug)
FTRC	Fail-to-Remain-Closed (leakage)
FRLO	Fail-to-Remain-Locked-Open
FRLC	Fail-to-Remain-Locked-Closed
FTOP	Fail-to-Operate
FTDP	Fail-to-Deliver-Power
FTT	Fail-to-Transfer

b. Source Key:

ASEP - Reference 1
EG&G CRBP - Reference 2
IEEE - Reference 3
IPRDS (valves) - Reference 4
IPRDS - (pumps) - Reference 5
IREP - Reference 6
LER (valves) - Reference 7
LER (pumps) - Reference 8
NREP - Reference 9
WASH-1400 - Reference 10

c. Certain failure modes were not used and no longer appear in the table. The corresponding event codes are:

10, 11, 21, 23-25, 34, 42-50, 83, and 106-110.

Table 2.2
Maintenance Screening Values

Maintenance Unavailabilities

	Event Code	Nom.	Source
Pumps - Motors (non-safety)	M2	3.0E-3	IPRDS MEAN[5]
(safety)	M1	1.0E-3	ASEP MEDIAN[1]
Pumps - Turbine	M3	1.0E-2	ASEP[1]
Valves - Motor-Operated Pneumatic, and Solenoid-Operated	M4	3.0E-4	ASEP[1]
Diesel Generator	M5	6.0E-3	NUREG/CR-2989,[11] IPRDS[12]
Batteries	M6	1.0E-3	IPRDS,[12] ASEP,[1] NUREG-0666[13]
Chargers	M7	3.0E-4	IPRDS[12]
Inverters	M8	1.0E-3	IPRDS[12]
Circuit Breaker	M9	6.0E-5	Calvert Cliffs PRA[14]
Relief Valve	M10	3.0E-4	Similar to M4
Bus	M11	6.0E-5	Similar to M9
ADS Actuation Circuit	M12	3.0E-4	Similar to M4
Heat Exchanger	M13	3.0E-4	Calvert Cliffs PRA[14]
ADS Control Circuit	M5	3.0E-4	Similar to M4
Strainers	M16	3.0E-4	Similar to M13
Fans	M18	5.0E-4	Calvert Cliffs PRA[14]
Motor Damper	M19	5.0E-4	Similar to M18
Damper Control Circuit	M20	1.0E-4	Event 102 * 3 * 10 hr

Table 2.2
Maintenance Screening Values (Concluded)

Maintenance Frequencies

	Event Code	Nom.	Source
Pumps - Motors (safety)	M1A	1.0E-4/hr.	ASEP[1]
(non-safety)	M2A	1.0E-4/hr.	ASEP[1]
Pumps - Turbine	M3A	3.0E-4/hr.	ASEP[1]
Valves - Motor-Operated, Pneumatics, and Solenoid-Operated	M4A	3.0E-5/hr.	IPRDS[4]
Diesel Generator	M5A	3.0E-4/hr.	NUREG/CR-2989[11]
Batteries	M6A	1.0E-4/hr.	IPRDS[12]
Chargers	M7A	3.0E-5/hr.	IPRDS[12]
Inverters	M8A	1.0E-4/hr.	IPRDS[12]
Circuit Breakers	M9A	8.0E-6/hr.	Calvert Cliffs IREP PRA[14]
Relief Valve	M10A	3.0E-5/hr.	Similar to M4A
Bus	M11A	8.0E-6/hr.	Similar to M9A
ADS Actuation	M12A	3.0E-5/hr.	Similar to M4A
Heat Exchanger	M13A	3.0E-5/hr.	Calvert Cliffs IREP PRA[14]
ADS Control Circuit	M15A	3.0E-5/hr.	Similar to M4A
Strainers	M16A	3.0E-5/hr.	Similar to M13A
Fans	M18A	7.0E-5/hr.	Calvert Cliffs IREP PRA[14]

Table 2.3
Test and Calibration Estimates

	Event Code	Nom.	Source
SBLC Test Pump	T1	1.0E-3	Assume 1 Hr. Test
SBLC Test Pump	T1A	1.4E-3/hr.	Tested 1 per Month
PCS Test (Quar.+Mon.)	T2	3.0E-3	Assume 2 Hr. Test
PCS Test (Quar.+Mon.)	T2A	1.4E-3/Hr.	Same as T1A
PCS Test (Shut+Mon.)	T3	3.0E-3	Same as T2
PCS Test (Shut+Mon.)	T3A	1.4E-3/Hr.	Same as T1A
PCS Test (Shut+Mon.)	T4	3.0E-3	Same as T2
PCS Test (Shut+Mon)	T4A	1.4E-3/Hr.	Same as T1A
DPS Test	T5	3.0E-3	Same as T2
DPS Test	T5A	1.4E-3/Hr.	Same as T1A
ADS Timer Cal.	T6	1.0E-3	Same as T1
ADS Timer Cal.	T6A	5.0E-4/Hr.	1/2 hr. duration
ADS Timer Fun.	T7	3.0E-3	Same as T2
ADS Timer Fun.	T7A	1.4E-3/Hr.	Same as T1A
RCIC Test	T8	3.0E-3	Same as T2
RCIC Test	T8A	1.4E-3/Hr.	Same as T1A
RPT Test	T9	6.0E-3	2 hrs each, level and pressure
RPT Test	T9A	1.4E-3/Hr.	Same as T1A
HPCS Test	T10	3.0E-3	Same as T2
HPCS Test	T10A	1.4E-3/Hr.	Same as T1A

Table 2.4
Internal Initiating Events

	Initiating Event	EPRI Categories	Nom.	Footnotes
1.	Turbine trip with turbine bypass available	1,3,14-21,27,29,30,33-37	5.0/Ry.	
2.	Turbine trip with turbine bypass unavailable	2,4,10,13	.5/Ry.	
3.	Total MSIV closure	5,6,7,9	.7/Ry.	
4.	Loss of normal condenser vacuum	8	.4/Ry.	
5.	Total loss of feedwater	22,24	.6/Ry.	
6.	Trip of one feedwater/condensate pump	23	.2/Ry.	
7.	Inadvertent opening of safety/relief valve (stuck)	11	.2/Ry.	
8.	Loss of offsite power	31,32	.1/Ry.	
9.	Loss of 125V DC Bus 2A or 2B (emergency power)		5.0E-3/Ry.	(d)
10.	Loss of 4160V AC Bus 241 or 242 (emergency power)		5.0E-3/Ry.	(e)
11.	Complete loss of instrument air		3.0E-3/Ry.	
12.	Complete loss of drywell pneumatic		3.0E-3/Ry.	
13.	Complete loss of 100 lbs. drywell pneumatic		3.0E-3/Ry.	
14.	Reactor vessel narrow range reference leg failures - all channels		3.0E-3/Ry.	

Table 2.4
Internal Initiating Events (Concluded)

	Initiating Event	EPRI Categories	Nom.	Footnotes
15.	Reactor vessel level narrow range reference leg failure - two channels		3.0E-3/Ry.	
16.	Small LOCA		3.0E-2/Ry.	
17.	Medium LOCA		3.0E-4/Ry.	
18.	Large LOCA		3.0E-4/Ry.	(a)
19.	Reactor vessel rupture		3.0E-7/Ry.	
20.	Steam line break		3.0E-3/Ry.	
21.	RHR suction, return, or injection line break		3.0E-5/Ry.	(b)
22.	CRD drive water line break (without isolation)		3.0E-7/Ry.	(c)

(a) The upper bound is based on 0 occurrences in approximately 275 reactor years of BWR experience and is representative of an approximate 90% confidence interval (to nearest half order magnitude).

(b) Analysis of valves in RHR line having internal leakage or unavailability due to previous catastrophic failure.

(c) Manual valve fail-to-close times rupture estimate based on no ruptures in approximately 275 BWR reactor years of experience.

(d) Values used in ASEP and deduced from NUREG-0666.

(e) Extrapolated from DC bus rates.

Table 2.5
Common Cause Beta Factors

Component	Mode	Nom.	Cons.	Sources
Diesel generators	FTS	.08		NUREG/CR-2099
	FTR	.07		(Ref. 15)
MOV	FTOP	.05	.03	NUREG/CR-2770
				(Ref. 16)
Check valves	FTOP	.06	.3	NUREG/CR-2770
	Internal leakage	.10	.7	(Ref. 16)
Relief valves	FTO	.13	.5	NUREG/CR-2770
	Internal leakage	.5	.7	(Ref. 16)
Pump (motor)	FTS	.06	.4	NUREG/CR-2098
				(Ref. 17)
Alt. motor-pump	FTS	.09	.4	NUREG/CR-2098
	FTOP	.04	.6	(Ref. 17)
Standby pumps	FTOP	.04	.5	NUREG/CR-2098
				(Ref. 17)
DC power		0.4		NUREG-0666
				(Ref. 13)

FTS - Failure to start
FTR - Failure to run
FTOP - Failure to operate
FTO - Failure to open

This brings up the problem, for components for which demand failure probabilities are given, of how much of the failures are really demand related and how much are rate dependent. For some components, the data base has demand failures but these were calculated for a set of components tested, say, monthly. A similar component tested only every refueling outage (i.e., every 18 months) might be expected to have a significantly higher failure probability. The actual difference in unavailabilities depends on the fraction of the root causes of the failures that are rate dependent. Not much work has been done in this area. Some information can be obtained by looking at the LER data reports[7,8,18-20] and examining the root causes listed for the failures (when they exist) and calculating the percentage that are thought to be rate dependent using engineering judgement for the classification.

The basic question is, "How should the failure rates for components tested only at very long test intervals be represented in the PRA?" For this analysis it was decided to use the upper bound of the distribution to represent the failure probability for those components which had only demand failure probabilities. Since the components that were tested infrequently were in the data base, it was judged that just converting the demand probability to a failure rate and calculating a new unavailability for the components tested over long intervals would lead to failure probabilities that were too large. Such large failure probabilities have not been observed and, if the model was true, they would have been observed even with the limited data that is available.

In the tables which follow, each event is assigned a letter code and a number code for its failure mode. For example, "Turbine-Driven Pump" has the code FTS for the failure mode fails-to-start. Some components have multiple failure modes which are classified into the same event code. For "Motor Operated Valve" on Table 2.1, the two failure modes Fail-to-Open (FTO) and Fail-to-Close (FTC) are considered to be the same failure mode of the component. They are both classified Fail-to-Operate (FTOP) and quantified with the same estimate. The number code for each failure mode is simply an internal accounting device for the RMIEP analysts. A number was assigned to each failure estimate for identification. With almost 300 events, it is often easier to refer to events by number than by name. This feature may be of interest to readers who wish to cross reference the paramecer estimations used in the final sequence quantification (Section 2.6) with the initial screening estimates here.

2.2.3 Notes on Screening Parameter Estimates

Component failure mode estimates are presented in Table 2.1. These failure modes involve actual hardware or electrical faults in the various components. In Table 2.1, the nominal value is the result of comparisons of values from many sources. Sources for the various component failure mode rates are included. Source references for the LER and IPRDS reports refer to the appropriate documents for each component type (e.g., Licensee Event Report [LER] valve,[7] pump,[8] or diesel generator[18] reports).

Component maintenance unavailabilities are in Table 2.2. Test and calibration contributors to component outages are in Table 2.3. Initiating events are listed in Table 2.4, and common cause failures are in Table 2.5.

Table 2.2 contains estimates of maintenance unavailabilities and maintenance frequencies. The class of components for which information is available is limited. The maintenance activities at a particular plant are likely to be heavily dependent on technical specifications and on the manner in which the maintenance personnel handle imposed time limitations. Because of this, it is difficult to generalize maintenance frequency and maintenance duration actions from plant to plant. The values in Table 2.2 are, however, consistent with estimates used in past PRAs. The values for the unavailabilities represent the product of maintenance frequencies derived from component failure rate data and the mean maintenance duration derived from various sources.

The values given in Table 2.4 for transients are derived from the data given in NUREG/CR-3862,[21] which is an update of EPRI NP-2230.[22] The nominal values reflect the average over the 25 BWR plants given. The conservative value reflects the amount of plant-to-plant variability in the data.

Potential common cause Beta factors are shown in Table 2.5. Values are taken from LER summary analyses in NUREG-2099,[15] NUREG/CR-2770,[16] and NUREG/CR-2098.[17] The screening analysis was limited to the use of common cause Beta factors. Beta factors are technically relevant only to common cause faults of two components. The application of Beta factors to three and four components is conservative. The method for calculating common cause failure probabilities involves the use of Beta factors. A Beta factor is a conditional probability that, given the failure of one component, one or more redundant components will fail. Common cause events are estimated as the product of a Beta factor and the appropriate component failure mode frequency.

2.2.4 Definition of Component Boundaries

Certain components such as valves, pumps, and circuit breakers rely on control, power, and actuation mechanisms in order to function properly. The boundaries of such components must be carefully defined so that data are not incorrectly associated with the various component failure modes. RMIEP is modeling components at a finer level of detail than most PRAs. The control, power, and actuation mechanisms of components are modeled separately from the actual component. In many data analyses, these mechanisms have been lumped together with the components. Failure rate estimates may be influenced by faults which are not relevant to the RMIEP component boundaries. In the screening quantification, this does not present a problem as conservative estimates are acceptable. But for the final quantification, the component failure rate estimates are refined to separate control, power, and actuation faults from the specific component faults. The component boundaries defined below are for components modeled at a finer level of detail than usual.

Pumps

The pump component is defined as the pumping unit, its prime mover, coupling, and associated mechanical controls. Pumps are classified by their prime mover, turbine-driven or motor-driven. Motor-driven pumps include the motor and the junction box between the motor windings and the power source. The turbine-driven pump includes the mechanical controls and governor, and lube-oil systems. The trip-throttle valve is the inlet boundary and the exit point of the turbine is the outlet boundary. The control circuit and actuation are modeled separately.

Valves

The valve component consists of the valve body and internal parts, the operator (motor, solenoid, and wheel), and any functional accessories such as limit or torque switches needed in order to function properly. Valves are classified by operator type - motor, air, solenoid, or manual. Check valves and safety relief valves are classified separately. The control circuit and actuation are modeled separately.

Circuit Breakers

The circuit breaker component consists of the actual mechanical device which can serve to disrupt the current in an electrical circuit. The control circuit and actuation are modeled separately.

Diesel Generator

The diesel generator component consists of the actual diesel and its immediate support (mechanical, air, and electrical) subsystems. The room cooling, DG cooling from the core standby cooling system (CSCS), the circuit breaker for loading onto the appropriate 4160 VAC bus and its control circuit, the diesel actuation and control circuitry are all modeled separately.

2.3 Fault Tree Event Models

Once screening values have been assigned to the various component failure modes and human actions, the fault tree basic events can be quantified to allow for screening quantification of the fault trees and accident sequences. At this step of the PRA, the uncertainty of the parameter estimates is not incorporated into the models. The screening of system and accident sequence models is performed by calculating point estimate values for the system fault trees and accident sequences. The purpose is to streamline the models to focus the analysis on potentially dominant failures and sequences. Uncertainty in the event occurrence rate or failure probability is incorporated in the final quantification.

There are five types of basic events in the fault trees. These are related to the six types of parameters in Section 2.2. These are:

1. Component failure events,
2. Common cause failures,
3. Test and maintenance unavailabilities,
4. Operational errors, and
5. Initiating events.

The various fault tree events in these categories and the methods used to quantify them using the parameter estimates evaluated in this task are described in this section.

The procedure used to actually construct the data base in a form for input into the SETS code,[23] which performs the fault tree and accident sequence solutions, consists of the following steps. First, a dBase[24] file was set up containing the generic data base with columns for the component type, failure mode, event code, nominal value to be used in the screening analysis, and notes on the source of the data. Second, another dbase file was set up containing all of the basic event names from all the fault trees grouped by system (3,450 events in all). This file contained columns for the event fault tree type, the event fault tree name, two columns for demand and rate types into which was put the event code for demand failures or failure rates or human actions, an estimate of the standby exposure time, and an estimate of the mission run time. Additional columns were calculated by a dBase program using the formula for transporting the failure rate and the demand failure probability from the generic data file to this file and then calculating the total unavailability. The last column contained system analyst notes on the particular component pertinent to its quantification. Third, a SETS Value Block was formed by writing the columns with the event name and total unavailability from the dBase file to a new file in SETS input format. This file was then used in the system and accident sequence analysis to evaluate the cut set probabilities and truncate the cut sets based upon cut set probability.

2.3.1 Component Failure Quantification

Most basic events were defined as individual components failing in a specific mode. However, logistical considerations permitted fault tree analysts to define several basic events as a single component with combinations of two or more failure modes, or as combinations of several components. This last type of event is referred to as a "Macro" or "Super" event. Each type of basic event is illustrated below.

2.3.1.1 Single Component - Single Failure Mode Events

Virtually all component failure modes defined by the fault tree analysis fit into two categories:

1. Failure to Start Function
2. Failure to Continue Functioning

2.3.1.1.1 Failure to Start Function

Events of this type involve components that must change status in response to an incident - such as a standby pump which must start, a valve which must change from open to closed - or components that are not in their proper status at the time their function is demanded. Basic events of this type are modeled as either demand related failures or failures that occur in standby.

The first model assumes that the probability of a component failing is constant depending only on whether the component is demanded. In Table 2.6, Eqn. 1, the quantification of this type of event is illustrated. The second model, failure-in-standby, assumes that failure could occur between demands. A constant standby failure rate, λ_s, and the average exposure time are used to calculate a failure probability. The exposure time of a fault tree event is the time interval between testing or verifying that the component functions and is in the correct state. LaSalle plant procedures were reviewed to find relevant exposure times for standby components. In Table 2.6, Eqn. 2, the quantification of this type of event is illustrated.

2.3.1.1.2 Failure to Continue Function

This type of component failure is associated with those components that must continue to function in a particular state throughout the plant response to an accident or transient event. This failure mode implies that the component has successfully changed state on demand or was properly aligned when demanded. The parameter estimations used here are in the form of operating failure rates (λ_o). Components must function for 24 hours, after which the accident is considered to be terminated. At 24 hours, the decay heat has dropped to a level where the success requirements of the systems are far more relaxed than what is modeled in the system fault tree models. Diesel generators are assigned a mission time of only eight hours, this was derived by convolving the probability of recovering loss of offsite power versus time curve with the DG integrated unavailability versus time curve to obtain the mean time interval over which the DG would be expected to operate. Furthermore, extraordinary recovery actions have high probabilities of succeeding in this time frame. The time of response is referred to as the mission time. In Table 2.6, Eqn. 3 the quantification of this type of event is illustrated.

2.3.1.2 Events With More Than One Failure Mode

Certain basic events were defined as the combination of a particular component's failure modes. As an example, failure of the High Pressure Core Spray pump to operate was modeled as one event, Fail-to-Operate, which is the sum of Fail-to-Start and Fail-to-Run. Such events are the combination of the two types of events discussed previously in Section 2.3.1.1. To quantify such combined failure modes, the point estimates of the individual component failure modes are quantified as in Table 2.6 and

Table 2.6
Quantification of Fault Tree Basic Events

Component Fails to Change State on Demand	$Q = Q_d$	(1)
Component Fails to be in Proper State when Demanded	$Q = 1/2 * \lambda_s * T_E$ (Exposure Time)	(2)
Component Fails to Continue Function	$Q = 1-\exp(-\lambda_o t_o) \simeq \lambda_o t_o$ for $\lambda_o t_o < 0.1$	(3)
Component Fails to Function Due to Human Error occurring in Maintenance	$Q = 1/2 * \lambda_m * T_E * HEP$	(4)
Component Fails to Function Due to Human Error occurring in Testing	$Q = \lambda_T * T_E * HEP$	(5)

simply added together. When probabilistic uncertainty is incorporated into the problem, the calculation is more complicated since two random variables are summed. This problem is discussed in Section 2.5 but is not a problem here since the screening analysis operates with point estimates.

2.3.1.3 Macro Events

Some events in the fault tree analysis were defined at a level of detail above the component level. These events are either modeled as "black box" or quantified as combinations of their individual components. Examples of black box events are the Reactor Protection System and the Gland Sealing System. Such events were quantified as 1.0 for the screening analysis.

Black box events, which were identified as potentially dominant in the screening analysis, were analyzed in more detail for the final quantification. An estimate of the failure probability for each black box event was calculated from the parameter estimations of the constituent components and relevant failure modes. Most black box events are plant subsystems for which fault tree analysis was either not useful or not necessary.

Some events were defined at a level below the black boxed subsystems but above the individual component level. An example of such an event is "Circuit Breaker - Fail-to-Remain Open." Although data exists for "Circuit Breaker - Failure to Open," information for "Failure to Remain Open or Closed" is not as usable. As a result, circuit breaker failures to open can be modeled specifically, but failure to remain in a certain state must be modeled as a combination of the components which actually make up the circuit breaker. A simplistic but realistic model of the event is constructed and quantified with the relevant component failure mode estimates.

2.3.2 Common Cause Failures

Common cause events for two similar components are quantified with Beta factors. A Beta factor is a conditional probability that a component will fail if a similar redundant component has failed. This method implies that some portion of the actual or potential failures observed in individual components represent mechanisms which act on all redundant components simultaneously. The Beta factors used in both the screening analysis and final quantification are calculated from analysis of component failure data which exhibited common cause characteristics.

There have been several extensive analyses designed to study data for common cause failures and to develop methods to quantify common cause events. This is an area of PRA in which efforts to resolve issues are continually frustrated by the nature of the problem. Section 2.4 discusses some of the problems encountered in common cause quantification. The Beta factors are used to quantify common cause events by multiplying a component

failure mode estimate by its appropriate Beta factor. For example, common cause failure-to-start for diesel generators is quantified as:

$$Q_{cm} = b_{dg} * Q(\text{Diesel Generator Fails to Start})$$

$$= 0.012 * 2.5E\text{-}2$$
$$= 3.0E\text{-}4$$

The above example is based on values used in the final quantification.

For more than two similar components, such as three or four parallel pumps, the Beta factor does not apply. However, a similar approach with a common cause factor which is the conditional probability that n components will fail given that a similar one has failed is used.

References 15, 16, 17, and 25 are the informational basis of the common cause factors. Details of common cause factor calculations are shown in Section 2.6.

2.3.3 Test and Maintenance Failures

There are two major contributors to test and maintenance outages of components:

1. A component is assumed to not be functional when it is being tested or maintained.

2. A component is not functional due to human error in performing the test or maintenance and returning it to service (i.e., failure to restore).

RMIEP has incorporated test and maintenance failures into the fault tree analysis at the component level. This is much more detailed than identifying maintenance outages only by system or subsystem.

The maintenance unavailability was calculated either by summing up the maintenance outage times and then calculating a yearly unavailability (fraction of time unavailable during operation) or by calculating a component failure rate (based on all failures not just catastrophic) and then multiplying this by a mean time to repair for the specific component type obtained from IPRDS data.[4,5,12] The maintenance frequency was also used in the calculation of operator failure to restore from maintenance by assuming that the component maintenance occurred at any time during the test interval and multiplying this by the conditional probability of the operator failing to restore. A similar formula was used for failure to restore from test except the component was assumed to be unavailable until the next scheduled test. Table 2.6, Eqns. 4 and 5, show the formulas for these calculations.

2.3.4 Initiating Events

The set of initiating events for the event tree analysis was established from past PRAs, industry analyses of transient events, and failure mode and effects analysis of LaSalle systems to determine the validity of support system transients as plant trips. The screening values for initiators were taken from past PRAs and industry analyses of transient data. For two initiators, no data exists. These initiators represent hypothesized events which have not been observed but are issues of concern. The initiators are two different pipe rupture scenarios in the reactor vessel narrow range indicators. These events were modeled as redundant pipe ruptures, and quantified with generic pipe rupture frequencies. Details of these calculations are in Section 2.6.

The screening transient estimates did not undergo significant change for the final quantification. The lack of plant specific data for LaSalle necessitated the use of generic transient estimates for the final quantification, which formed the basis of the screening analysis. Annual updates of industry transient experience were reviewed to incorporate the most recent information.

2.4 Discussion of Data Analyses and Parameter Estimation Studies

In this section, the various sources reviewed to arrive at a final set of parameter estimates for the accident sequence quantification are discussed. The actual details and results of the reevaluation of parameter estimates are discussed in Section 2.6.

The ideal situation for parameter estimates is to statistically analyze plant specific data. This would ensure that the resulting estimates represent the effects of factors specific to the operating environment of the modeled components. These factors include maintenance practices, installation, test procedures, staff training, component manufacture, and the environment (clean, dirty, dry, humid). LaSalle is a very new plant with little operating experience available. Even older plants do not offer sufficient plant specific data to properly quantify the majority of parameter estimates needed for a PRA analysis at the level of RMIEP. For this reason, generic parameter estimations based on industrywide data is used extensively. Such analysis greatly increases the pool of information from which component behavior can be evaluated. A problem with generic parameter estimates is that factors not relevant to a specific plant may be imposed on models of that plant. Generic data analyses by no means represent a complete solution to the problem of parameter estimation but, in lieu of extensive plant specific information, they are a workable tool.

As generic parameter estimates formed the bulk of RMIEP's final parameter estimation, the major effort in reevaluating the screening values was to review analyses of industry data and evaluate the applicability of these studies for RMIEP. RMIEP was not commissioned as a data collection and analysis program itself. Some data analysis was performed under the scope of the RMIEP analysis of LaSalle, and this will be discussed here as well.

Data collection of component failure information has not kept up with the development of PRA models. PRA models have progressed to a level of sophistication and detail that can accomodate accurate, detailed data. Past data analyses have rarely been coordinated with PRA programs to ensure component and failure mode definitions which are compatible to those in PRA models. Methods of recording component failures at most plants are not geared towards generating the type of information needed for useful PRA data analysis.

Some of the difficulties often encountered with data records are:

1. Description of failures are vague, even misleading,
2. Failure modes are not identified,
3. Operating hours of standby components are not recorded,
4. Successful demands of components are not recorded, and
5. Human faults are often concealed (the instrument was simply found to be nonfunctional - "reason unknown").

The references, in Section 2.7, are the list of documents reviewed for the RMIEP parameter estimation analysis. Specific comments on these reports follow.

2.4.1 Licensee Event Reports

The NRC assigned EG&G Idaho to perform data analyses of various component failures based on reviews of LERs submitted to the NRC by nuclear power plant operators. EG&G published several reports, five of which were reviewed for RMIEP parameter estimates. These reports, References 7, 8, 18, 19, and 20, investigated LERs for pumps, valves, diesel generators, relays, circuit breakers, and instrumentation and control components. The studies reviewed LERs from the early to mid-1970s up to the early 1980s.

The EG&G LER summaries present generic estimates of component failure mode parameter estimates. Confidence limits on the mean value estimates are given but uncertainty distributions that represent the range of observed values were not developed. It is incorrect to use the confidence limits on the mean value as upper and lower bounds on an uncertainty distribution that is supposed to represent the total range of values since it only represents how confident you are that the mean value is within a certain range. EG&G indicates that the values published are gross constant failure rate estimates and should be taken as tentative. Inadequacies of the LER system (e.g., vague descriptions, failure to report all faults) necessitated subjective judgement of LER events by the analysts. Information provided in the summaries is difficult to accurately assess. The methods of calculating the estimates are included in the reports, but the data used is presented in such a complex fashion so as to make it very difficult if at all possible to reproduce the parameter estimates.

Results of the LER summaries sometimes are confusing. For example, Table 15 of the valve report[7] lists a value of 6.0E-8/hr. for "MOV-Plugged"

(Failure-to-Remain-Open). This value is defined as involving command faults only. No hardware failure estimate is given for "MOV-Plugged." But the footnotes of the table state that the command failure estimate is derived from no recorded failures. How command failures and hardware failures apparently can be analyzed differently for either mode when no recorded failures exist is not illustrated in the evaluation methods of Appendix A of the report.

2.4.2 IPRDS Data Analyses Reports

The In-Plant Reliability Data Base for Nuclear Plant Components (IPRDS) is a data collection and analysis program performed for the NRC by Oak Ridge National Laboratory. The IPRDS program was specifically redirected, for the purpose of supporting the LaSalle analysis, to analyze two additional BWRs that were deemed to be, in some ways, similar to LaSalle. Three reports were reviewed for RMIEP, References 4, 5, and 12. These are the IPRDS reports for valves, pumps, and diesel generators, batteries, chargers, and inverters. The reports utilize data from two PWR units and four BWR units for pumps and valves, and five unspecified plants for diesel generators.

As with the LERs, the IPRDS reports present estimates for component failure modes and associated confidence limits, but no probability distributions. The IPRDS method of data collection involves accounting for total component operating time and number of demands. However, it is not clear how accurately this information can be learned from plant records.

2.4.3 LANL IPRDS FRAC Analysis

As part of RMIEP, a portion of the IPRDS effort was directed to Los Alamos National Laboratory (LANL). The purpose of this was to "simulate" plant specific data analysis by analyzing data from two BWR plants considered to be similar to LaSalle. LANL also performed analyses on data from all four of the IPRDS BWR plants and both PWRs.

LANL maintains and operates the Failure Rate Analysis Code (FRAC).[26] This code allows factors such as plant, system, operator type (drive mechanisms), mode of operation, size, and type of component to be analyzed for effect on failure rates. Reference 27 summarizes the LANL analysis. The study's aim was to identify those factors in the IPRDS data base which affect failure rates, how the factors affect the failure rates, and to calculate failure rates with both confidence and tolerance intervals.

The LANL analysis yielded failure rate adjustment factors which were calculated for the various factors identified for each component. These adjustment factors are applied to an average failure rate estimate for each type of component. The LANL analysis was restricted to pumps, valves, and diesel generators.

The LANL FRAC analysis did not prove very useful in a practical sense to RMIEP, although it was a valid initial step in establishing a process of analyzing data for detailed failure rates. The LANL analysts feel that gaps in the data render a reliable FRAC analysis impossible. Component boundaries and failure mode definitions in the IPRDS data given to LANL were inconsistent with the needs of RMIEP.

2.4.4 General Electric LaSalle Probabilistic Safety Analysis

General Electric performed a probabilistic safety analysis of LaSalle.[28] Their analysis is based mostly on their own standard probabilistic analysis of BWR/6 plants, called GESSAR II. This standard analysis was revised to be specific to LaSalle.

The parameter estimates used in this report represent a collection of values from numerous NRC and industry sources. The GE analysis used estimates from sources such as WASH-1400, various NUREG reports, IEEE-500, NPRDS, and several General Electric reports. Mean estimates were used. No probabilistic uncertainty was incorporated into their parameter estimates. Several values used in the GE study were close or even equal to values used in the RMIEP analysis, but several values were significantly lower than those found in other studies. No explanations were given for GE's selection of failure rates.

RMIEP analysts met with General Electric reliability analysts who worked on the GE LaSalle study to investigate the potential sources of GE data. GE has an extensive data base of component failures from their nuclear plant customers worldwide. The data base is continuously updated. However, no data analysis relevant to PRA appears to be ongoing. GE did not use this data base for their LaSalle study.

2.4.5 Transient Data Analyses

Two studies provided significant analysis of industry-wide transient data for parameter estimates. Reference 29, NSAC-103, is an EPRI update of loss of offsite power transients, and Reference 21, NUREG/CR-3862 is an EG&G analysis of several types of transient events. NUREG/CR-3862 provides uncertainty intervals of parameter estimates, but does not study probability distributions based on the data. NSAC-103 does not treat parameter uncertainty. Both reports present their analyses clearly. Their results are easily reproducible.

2.4.6 Other Parameter Estimation Sources

The remainder of the references primarily are sources of generic estimates that draw on judgement, engineering analysis, or other analyses of data. Two significant exceptions are Reference 11, NUREG/CR-2989, which is a data

analysis of diesel generator failures at nuclear power plants, and Reference 25, EPRI NP-3967, an analysis of common cause failures in nuclear power plants. NUREG/CR-2989 utilized LERs and questionnaires to Licensees to accumulate information. This report was very useful for parameter estimates and uncertainty characterization for diesel generators and related components. The EPRI report formed the basis of the RMIEP common cause quantification. This report reviewed and classified events from Nuclear Power Experience,[30] a monthly updated compilation of failures and unusual occurrences published for the nuclear industry. This report is reviewed in more detail in the common cause discussion of Section 2.6.

An additional source of common cause information is a search of maintenance work requests for LaSalle 1 and 2 by Oak Ridge National Laboratory. This unpublished analysis was done for RMIEP and accumulated information in a data base for application with Fleming's common cause methodology in EPRI NP-3967.[25] No common causes were found.

Two other sources, that were used extensively in RMIEP, are the IREP Procedures Guide,[6] and the Energy Incorporated (EI) PRA data survey.[31] Both reports are useful because of the large number of component failure modes for which they provide estimates. The IREP report represents the opinion of experts for many estimates and does not necessarily incorporate values based on data. The IREP values tend to be conservative; however, many IREP parameter estimates compared well with values from analyses such as the LER summaries, IPRDS, and the GE LaSalle Safety Study.

The EI data survey represents the results of a review of several parameter estimation sources as part of EI's work on the Monju PRA.[32] The PRA is proprietary, but the data survey only includes information used to guide the PRA, and not necessarily used in it. The survey reviewed a variety of data analyses and other PRA related reports, including IPRDS, LER summaries, IEEE-500, WASH-1400, and the IREP Procedures Guide. The EI data survey lists a mean parameter estimate and an error factor based on a lognormal distribution for each component failure mode. In the EI data survey, it is assumed that all parameter estimates from all studies are lognormally distributed. The EI data survey actually is more than just a review of the various sources. There is some manipulation of information from the reports surveyed. It is important to understand that the information in the EI data survey may not exactly correspond to the information in the original reports.

2.5 Characterization of Parameter Estimate Uncertainty

For the final quantification of the RMIEP accident sequence models, the uncertainty of the parameter estimates is incorporated in the models. This is accomplished by characterizing the parameter estimates as random variables. Each basic event appearing in the final models is linked to one of the basic parameter distributions and can be correlated at any level desired. These distributions go into the Latin Hypercube program[33] which

generates a stratified sample containing, for the LaSalle analysis, 400 sets of observations each containing a value for all of the variables used in the final quantification. For each sample member, a value for each accident sequence is calculated, yielding a distribution of values for the accident sequence models generated from the uncertainty of the parameter estimates used in the models.

Historically, PRA has most commonly characterized uncertainty with lognormal distributions. The mean value of the distribution is used as a point estimate of a parameter's value and is used for point estimate calculations of the sequence models. The lognormal distribution is popular because many components and devices for many different industries seem to display failure behavior which fits the lognormal model well.

RMIEP is utilizing sampling methods in the sequence quantification which permit parameters to be modeled by any of several types of distributions. However, the data analysis methods used in the reports reviewed for this analysis do not generate distributions for parameter estimates. Confidence intervals are sometimes calculated, but they do not necessarily give insights on a parameter's probability distribution. In some of the data analyses, no parameter uncertainty ranges are calculated.

RMIEP reviewed the data analyses and PRA reports listed in the references. From these reports, a best estimate of a parameter's value was established. This value was assumed to be the mean value of the parameter's distribution. If information regarding a parameter's distribution and range of values existed in any of the reports, it was used in the parameter estimation model. Otherwise, the parameter's distribution was assumed. The range of a distribution was based on uncertainty information on the parameter estimate. The lognormal distribution was the predominant distribution used for the RMIEP parameter estimations.

Some basic events are defined as the combination of two component failure modes. For example, failure of a motor-driven pump to operate is a combination of "Motor Pump Fails-to-Start" and "Motor Pump Fails-to-Run." The actual random variable which should be sampled for this combination is the sum of the two constituent random variables. The computer sampling programs used in RMIEP allow this to be done. In the sampling routine, both individual failure modes are defined as random variables based on the review of data analyses and are sampled separately. The combined event is also defined as a random variable in the sampling routine. It is defined as the sum of the two individual failure modes. The routine will construct a random sample of the combined event by using the samples of the two individual failure modes in the relationship defined by the combination (i.e., the sum of the two individual failure modes).

2.6 Parameter Estimates For final Quantification

In this section, the results of the final parameter estimates and their uncertainty models are presented. The sources of the information used are

in the reference list for this chapter. The results are discussed for each component failure mode and initiating event used in the final quantification. The set of component failure modes for the final quantification has been greatly reduced due to results of the screening analysis. The initial set defined by the system fault tree analysis generated almost 300 separate component failure modes and initiating events. Failure combinations which are below certain threshold levels in the fault tree screening and accident sequence screening analysis were deleted. The number of component failure modes relevant to the remaining basic events was reduced to approximately 70. This demonstrates the utility of screening techniques for vastly streamlining problems.

The results are summarized on Tables 2.7 through 2.14. For each component failure mode, its screening parameter estimate is shown, along with estimates from the various sources, and the parameter model chosen for RMIEP.

The component failure code number is also included on the tables. This will facilitate comparison of the final parameter estimates to the initial screening estimates in Section 2.2. Each component failure mode is discussed in the text to explain the selection of the RMIEP models. The component failure modes have been classified into the following categories:

1. Pump Hardware Failures,
2. Valve Hardware Failures,
3. Electrical Component/Electrical Power Failures,
4. Miscellaneous Component Failures,
5. Maintenance Failures,
6. Initiating Events, and
7. Common Cause Failures.

2.6.1 Pump Hardware Failures

Standby Motor Driven Pump Fails on Demand - Fails to Start

The LER data summary by INEL (NUREG/CR-1205, Revision 1)[8] appears to be the only analysis which separates command failures from actual pump faults. This is consistent with the failure mode models used in RMIEP, which allow for recovery of the pump control circuit, but not for pump hardware failure. The pump component for RMIEP is defined as the pumping unit, its prime mover, the coupling between these, and mechanical controls. The LER summary definition is the same.

Any failure outside the boundary of the defined component would be a command failure. The value used in the GE LaSalle analysis - 3.2E-4/d - appears to be close to the value derived from INEL's LER summary. However, the reference for GE's value is the original NUREG/CR-1205,[34] and it is supposedly taken from page 420 of that document. The value given there is 3.2E-3/d, not 3.2E-4/d. It appears that the GE value may be in error.

The consistency between the various sources for Motor Driven Pump Failure-On-Demand in Table 2.7 - with command failures included - suggests that the data has been reasonably well analyzed, and that misinterpretation of pump failures is minimal. As the INEL LER summary is the only report which separates control faults from hardware faults, it is used as the basis of the RMIEP analysis. As seen on Table 2.7, the sources which include command faults in their estimates have values for pump-failure-to-start on the order of 1.0E-3/d and higher. Whereas the LER summary estimate without command faults is 4.0E-4/d. Separating command failures from pump hardware failures appears to be a significant distinction in failure modes. This failure mode estimate is modeled as:

Lognormal,
Mean - 4.0E-4/d,
Error factor - 10.

Standby Motor Driven Pump - Fails to Run

The failure model used here is from IREP.[6] The mean value (3.0E-5/hr.) is slightly higher than the value used in the GE LaSalle study (9.6E-6/hr.). The GE number is based on the original LER summary on pumps by INEL (NUREG/CR-1205). That report has been revised, but in the revision as well as the original, this failure mode is modeled for normally operating and alternating pumps only. Standby pump operating failure rates were not calculated. In the IPRDS analysis, the same is true. The reason why running failure rates for standby pumps have not been calculated is that these pumps, by definition, never operate, especially in the absence of accidents. Actual operating times from tests are not recorded for standby pumps. It is assumed here that standby motor pumps behave similarly to normally-operating pumps, and that the data from operating pumps applies. The model is:

Lognormal,
Mean - 3.0E-5/hr.,
Error factor - 10.

Standby Turbine Driven Pump Fails on Demand - Fails to Start

GE does not have this failure mode in their LaSalle analysis. The value from the Los Alamos analysis of IPRDS data using FRAC, 8.0E-4/d, is much lower than other sources. However, the authors of that analysis question the validity of the actual event estimates due to a lack of data available to them. This failure mode involves actual pump faults, no command failures. The LER value - 1.0E-2/d - is specifically based on pump failures only. The IREP value is only slightly higher - 3.0E-2/d. The model is:

Lognormal,
Mean - 3.0E-2/d,
Error factor - 10.

Standby Turbine Driven Pump - Fails to Run

The basis of this model is plant-specific data from the Peach Bottom Unit 2 BWR.[35] There is evidence which suggests that past data analyses have used reactor operating hours to model run time for standby turbine pumps. This is inappropriate for standby pumps, such as RCIC pumps, since the actual accumulated run time would be much less than the total reactor hours. It should be noted that there has been no excessive amount of turbine pump failures observed at Peach Bottom compared to other plants. The higher running failure rate for Peach Bottom on Table 2.7 is due to a change in the way the operating hours have been defined. The GE LaSalle study did not include this failure mode.

The turbine pump used in LaSalle's RCIC system is different than the turbine pumps at Peach Bottom. Commonwealth Edison has equipped the LaSalle plant with state-of-the-art components. Unfortunately, data on component performance does not exist for LaSalle, and the Peach Bottom analysis is the best available representation of turbine pump unavailability. The model is:

Lognormal,
Mean - 5.0E-3/hr.,
Error factor - 10.

2.6.2 Valve Hardware Failures

Motor Valve Fails-to-Remain-Open

Information on MOVs failure-to-remain open was not consistently analyzed in the various studies. The IPRDS estimate is based on PWR data, but is very close to the IREP value used for all valve types and plant types (2.0E-7/hr. compared to 1.0E-7/hr.). The LER summary was very unclear with respect to this failure mode. The LER value of 6.0E-8/hr. is based on no observed failures. Yet, an estimate is given only for command failures and none for hardware faults. With no observed failures, one might assume that MOV command and hardware failures would be treated similarly. No explanation is given for the LER estimates. WASH-1400 presents a demand probability estimate for this failure mode which was used in the GE LaSalle study. It is not shown exactly how this value was used for a time related failure. The RMIEP model for this failure mode is based on IREP:

Lognormal,
Mean - 1.0E-7/hr.,
Error factor - 3.

Motor Valves Fail-to-Remain-Closed

IPRDS presents a value of 2.0E-7/hr. for a failure mode called internal leakage. This is the only IPRDS failure mode possibly relevant here. The

IPRDS value is fairly close to the IREP value (2.0E-7/hr. compared to 5.0E-7/hr.). The LER summary did not calculate an estimate for this failure mode, and the GE LaSalle study did not use this failure mode. The IREP model has a very high error factor of 100. No reason for such an unusually high uncertainty is given. The upper confidence limit in IPRDS is a factor of 10 greater than the mean. The RMIEP model conservatively uses the IREP mean, but used an adjusted error factor due to insights presented in IPRDS:

Lognormal,
Mean - 5.0E-7/hr.,
Error factor - 10.

Air Valve Failure-to-Remain-Open

Information on this failure mode is limited. The IPRDS value of 7.0E-8/hr. is based on zero observed failures. The LER summary did not evaluate AOVs for this failure. IREP does not distinguish between valve types for this failure mode. The GE LaSalle study did not use this failure mode. The IREP model is used as the RMIEP model:

Lognormal,
Mean - 1.0E-7/hr.,
Error factor - 3.

Air Valve Failure-to-Remain-Closed

IPRDS presents a value of 2.0E-7/hr. based on no observed failures. The LER summary and GE LaSalle reports do not have estimates for this failure mode. The IREP model is used here:

Lognormal,
Mean - 5.0E-7/hr.,
Error factor - 10.

Check Valve, Failure-to-Remain-Open

This is a time-related failure mode similar to AOV and MOV fail-to-remain-open. Very little information is available for this failure mode. Only the ORNL IPRDS analysis of valves and the Energy Incorporated Data Survey mention this failure mode. The ORNL study defines a time-related check valve failure mode for plugging, but does not present any analysis of that mode. The Energy Incorporated Data Summary[31] presents a value of 1.6E-7/hr. for plugging based on the NPRDS. This value is somewhat higher than the mean estimate for AOVs and MOVs fail-to-remain-open of 1.0E-7/hr. However, the Energy Incorporated value is not well documented, so the model for this failure mode is from IREP, the same as for AOVs and MOVs:

Lognormal,
Mean - 1.0E-7/hr.,
Error factor - 3.

Check Valve, Failure to Operate

The INEL LER summary presents a value of 8.0E-5/d for GE plants. This is close to the IREP mean value of 1.0E-4/d, and the GE LaSalle value of 1.0E-4/d, which is from the original INEL LER summary. Therefore, the model used here is based on IREP:

Lognormal,
Mean - 1.0E-4/d,
Error factor - 3.

Motor Operated Valve Failure-to-Operate

This failure mode is either failure-to-open, or failure-to-close on demand. The calculated failure probabilities from ONRL's IPRDS and INEL's LER summaries straddle the IREP mean value of 3.0E-3/d. The LER value is 6.0E-3/d, and the IPRDS value is 5.3E-4/d. However, these studies appear to include control circuit failures in their estimates for this failure mode. RMIEP separates control circuit failures from component hardware failures. The RMIEP control circuit failure-to-operate estimate is 2.5E-3/d. The RMIEP MOV hardware failure-to-operate is estimated by subtracting the contribution of control circuit faults from the IREP estimate for MOV failure-to-operate:

MOV-FTO = 3.0E-3/d - 2.5E-3/d
= 5.0E-4/d.

The RMIEP model is:

Lognormal,
Mean - 5.0E-4/d,
Error factor - 10.

Manual Valve Fails-to-Remain-Open

IPRDS has a mean value of 6.0E-8/hr. which is close to the IREP value for all valves of 1.0E-7/hr. The EI data survey lists a value of 2.2E-8/hr. credited to NPRDS. The IREP model is used here:

Lognormal,
Mean - 1.0E-7/hr.,
Error factor - 3.

Solenoid Valves Fail-to-Remain-Open

The IPRDS study has a parameter estimate of 7.0E-8/hr. based on no observed failures. The EI data survey lists a value of 3.0E- 8/hr. credited to NPRDS. The IREP model for all valves is used here:

Lognormal,
Mean - 1.0E-7/hr.,
Error factor - 3.

Safety Relief Valve - Failure to Reclose

The INEL LER summary on valves presents an analysis of BWR primary relief valves. Their analysis yields an estimate of 3.1E-3/d with a 95% confidence limit of 4.7E-3/d, and a 5% confidence limit of 2.1E- 3/d. This is significantly different than the IREP model with a mean of 3.0E-2/d, error factor of 10. The GE LaSalle study used 0.01 to model this failure mode. The design of the LaSalle Safety Relief Valves is quite different than those at other BWRs. Commonwealth Edison has data on SRV testing and this data was evaluated to ascertain if other data analyses were relevant to LaSalle's SRVs. The LaSalle data showed no failures in 1200 SRV demands. This yields an estimated mean of 8.3E-4/d and a 95% confidence limit of 4.0E-3/d based on a binomial model of (0+1)/(1200+1).

The LaSalle data and the LER summary yield fairly close results and indicate low uncertainty of the estimate. The model for RMIEP is:

Lognormal,
Mean - 8.3E-4/d,
Error factor - 3.

2.6.3 Common Cause Factors

The RMIEP final quantification involves common cause failures of: the LPCI pumps, the MOVs in the LPCI system, the diesel generators, the diesel generator cooling water pumps, and the DC power system batteries. Other common cause failures were considered in the early systems analysis but did not survive the screening analysis. Several analyses have studied and classified component failure reports for common mode phenomena. The process of classifying events is fraught with problems. Failure reports are often very vague and must be reviewed with great subjectivity. Most analyses of common cause events generate debate regarding whether or not their identification and classification of common cause failure is accurate or complete.

Common cause analyses often fail to distinguish between failure modes of components (e.g., fail-to-run versus fail-to-start, open versus closed). Events have been classified as common cause when it is not clear that they should be. For example, two similar valve failures in different parts of the same system or even different systems do not necessarily imply a common cause phenomena. Yet, such events have been classified as common cause. Without reviewing such events in the context of system configurations, it is very difficult to evaluate events for potential common cause impact.

Events classified as common cause events in several studies (References 15, 16, 17, and 25) were reviewed.

The analysis of data needed to quell any apprehensions of inadequate common cause analysis would require excessive rework and effort far beyond the resources of RMIEP. The models used for RMIEP are based on the studies selected for the various common cause events. Reanalysis of the data was not done.

Pumps and Valves

The common cause analysis for pumps and valves is based on the work of Fleming.[25] The method for calculating Beta factors was retraced by applying the common cause data presented in that document to Beta factor equations. The generic values listed in Reference 25 do not always agree with the values calculated by using the data tabulated in the report. The discrepancy cannot be accounted for. The calculated values were used in RMIEP.

The Beta factors based on Fleming's work are for systems of two redundant components. In Reference 25, Fleming also presents a method for extending common cause analysis to multiple component systems, but no such analysis of the data is presented. For multiple component systems in RMIEP, the Beta factors based on Reference 25 are adjusted with appropriate multiple component failure rate factors based on Atwood's work (References 16 and 17).

LPCI and CSCS Pump Common Cause

Reference 25, an EPRI analysis of common cause failures, is the basis for the RMIEP model. The CSCS is a standby cooling system important for cooling the diesel generators. The EPRI report only analyzed standby RHR or LPCI pumps for common cause failures. The CSCS pumps and LPCI pumps are grouped together for common cause analysis. Using the data and the method for calculating Beta factors in Reference 25, a mean estimate of 0.15 was calculated. The value shown in Table 3-37 of Reference 25 is 0.11. The discrepancy cannot be accounted for. Confidence limits calculated with a binomial computer are very tight.

Confidence Limits	.05	Mean	.95
Beta Factors	0.1	0.15	0.26

Using multiple component failure rates from Reference 17, the Beta factor is adjusted to represent a 3 of 3 pump common cause event:

Lognormal,
Mean - 0.11,
Error factor - 3.

LPCI MOV Common Cause

Using the data and method presented in Reference 25, a Beta factor of 0.05 was calculated. The value reported in the report is 0.08. The discrepancy cannot be accounted for. Binomial confidence limits for the data suggest a very small distribution for the Beta factor:

Confidence Limits	.05	Mean	.95
Beta Factors	.04	0.05	.06

The MOV Beta factor is adjusted with multiple component failure rates from Reference 16. The model is:

Lognormal,
Mean - 0.03,
Error factor - 3.

Diesel Generator Common Cause

The diesel generator common cause Beta factor is from a calculation performed by Dale Rasmuson of the NRC (unpublished). The model is:

Lognormal,
Mean - 0.012,
Error factor - 3.

DC Power Battery Common Cause

The battery common cause Beta factor is from Reference 13, the DC Power Study - NUREG-0666. That report has a basic value of 0.4 for the Beta factor. That value is for their basic, minimum power system. A set of criteria in the report are used to evaluate any improvement factors for which a plant can be credited. An improvement factor of 0.1 is used for LaSalle based on improved maintenance and testing compared to the minimum system and the elimination of bus tie breakdown in LaSalle's DC system. The RMIEP model is:

Lognormal,
Mean - 0.04,
Error factor - 3.

2.6.4 Electrical Component Failure Rates

Circuit Breaker Failure to Operate

Failure-to-open and failure-to-close are treated as equivalent failure modes in RMIEP. The INEL LER summary on protective relays and circuit breakers presented values for failure-to-open and failure-to-close separately. The component failure modes were further divided into categories by NSSS vendor, function (e.g., Diesel Generator Output, Load Breaker), and voltage level - see Tables 10 and 11 of Reference 19. The voltage levels used to distinguish circuit breakers in Table 11 of the LER summary were medium and low. No actual voltage levels were defined. The utility of this information is limited and the categorization of circuit breaker faults by voltage levels was not used.

Table 10 of the LER report shows failure-to-open probabilities for diesel generator output breakers - 1.4E-4/d, and load breakers - 3.1E-5/d. These

two values are fairly different from each other and are significantly less than the IREP mean value of 3.0E-3/d. For failure-to-close, the LER values for DG output and load breakers, 7.0E-4/d and 8.8E-5/d, are higher than for failure-to-open. An hourly failure rate is calculated for feeder breakers - 1.6E-7/hr.

It is not clear how reliable the LER information is. Tables 10 and 11 of that report also present values for a failure category called Improper Operation. This failure category was defined in the LER summary to evaluate all LERs which could not be clearly identified as failure-to-open, failure-to-close, or spurious operation.

IREP and the EI data survey have values that are fairly close. However, as with MOV failure-to-operate, the sources of these values seem to include control failures in the parameter estimate calculations. The RMIEP circuit breaker hardware failure value is calculated by subtracting out the contribution of control circuit faults from the IREP value:

$$\text{Circuit Breaker FTO} = 3.0\text{E-}3/\text{d} - 2.5\text{E-}3/\text{d}$$
$$= 5.0\text{E-}4/\text{d}$$

The RMIEP model is:

Lognormal,
Mean - 5.0E-4/d,
Error factor - 10.

Circuit Breaker Failure to Remain Open or Closed

The INEL LER summary presents values for failure-to-remain-open separately from failure-to-remain-closed. Breakers are categorized by breaker type as well - DG output, feeder, and load breakers. The values presented in Table 10 of that report are approximately an order of magnitude less than the WASH-1400 value of 3.0E-6/hr., and the EI data survey value of 2.9E-6/hr. IREP has a demand-related probability of 1.0E-5/d. The LERs used to evaluate this failure mode suffer from the same problem as for Circuit Breaker, Failure-to-Operate. It is not always clear which failure mode a particular circuit breaker LER actually belongs to. For this reason, WASH-1400 is the basis of our model. The conservatism is acceptable in view of uncertainties regarding the LERs. Our model is:

Lognormal,
Mean - 3.0E-6/hr.,
Error factor - 10.

Diesel Generator - Failure to Start

With the exception of ORNL's IPRDS value of 3.0E-3/d, other sources show a strong consistency in estimation of this failure mode - approximately 3.0E-2/d. The AC power study, Reference 11, gives an overall value of 2.5E-2/d. In that study, plant-specific values for CECO plants compare closely to

that value - Dresden 2 and 3 have 5.1E-2/d, Quad Cities has 1.6E-2/d. Reference 11 includes output circuit breaker faults within the diesel generator boundary. This component is modeled separately in RMIEP. However, the contribution of output breaker faults to overall diesel generator unavailability in Reference 11 is insignificant. The plant-to-plant variation in the AC power study tends to be low. An error factor of 3 seems appropriate on an assumed lognormal distribution. The model used here is:

Lognormal,
Mean - 2.5E-2/d,
Error factor - 3.

Diesel Generator - Failure to Run After Start

There is strong agreement between the various sources reviewed for this failure mode. The AC Power Study has a value of 2.4E- 3/hr., which is very close to the IREP mean of 3.0E-3/hr. The AC Power Study is used as the basis here:

Lognormal,
Mean - 2.4E-3/hr.,
Error factor - 10.

Diesel Generator Control Circuit

Reference 11 identified 14% of all failures as control circuit failures. No information was given to separate control circuit failures between Failure-to-Start or Failure-to-Run. It was assumed that for each failure mode, the parameter estimate value was 14% of the appropriate diesel generator failure mode:

Failure-to-Start	Lognormal, Mean - 3.5E-3/d, Error factor - 3.
Failure-to-Run	Lognormal, Mean - 3.5E-4/hr., Error factor - 10.

Relay Failure to Energize or Re-energize

The INEL LER summary on relays does not analyze this failure mode. GE presents a value of 4.0E-7/hr., but discussions with GE reliability personnel have revealed that this value is in error. The EI data survey presents an hourly failure rate for spurious operation of 1.5E-7/hr. The IREP model for relay coil failure is used here:

Lognormal,
Mean - 3.0E-6/hr.,
Error factor of 10.

Contact Pair - Failure to Open or Close

There is not abundant information on this component failure. The EI data survey has a value of 5.3E-7/d, which is substantially lower than the IREP mean value of 3.0E-4/d. The IREP model for relay contacts is used, and the potential conservatism is acknowledged:

Lognormal,
Mean - 3.0E-4/d,
Error factor - 10.

Contact Pair - Spurious Opening

Spurious opening of contact pairs is equated to the WASH-1400 failure mode of Opening-of-Normally-Closed-Contacts. The EI data presented a failure mode listed as - Relays-Spuriously Open. The value shown there is 1.7E-6/hr. However, the EI survey claims that this value should be reduced by an order of magnitude for contact pair failures. The WASH-1400 model is used here.

Lognormal,
Mean - 1.0E-7/hr.,
Error factor - 3.

Contact Pair - Spurious Closing

This failure mode is equated to the WASH-1400 failure mode - Short-Across-Normally-Open-or-Normally-Closed-Contact-Pairs. Just as with Contact Pair - Spurious Opening, the EI data survey presents a value of 1.7E-6/hr. for spurious closing with a multiplication factor of 0.1 for contact pair failures. The WASH-1400 model is used here:

Lognormal,
Mean - 3.0E-8/hr.,
Error factor - 10.

Transformer Failure-to-Deliver-Power

All three sources which refer to this failure mode, WASH-1400, IREP, and the GE LaSalle study, use the same model:

Lognormal,
Mean - 1.0E-6/hr.,
Error factor - 3.

2.6.5 Miscellaneous Failure Modes

Dampers - Failure to Operate (Damper Fails to Open or Close)

IREP has a value of 3.0E-3/d for Damper Motor fails-to-operate, but there seems to be no reason why dampers and fans should not have similar electric

motors. WASH-1400 has a mean value of 3.0E-4/d for Fan Motor fails-to-start. The EI data survey lists a value of 2.7E-5/d credited to IEEE-500. The RMIEP model is based on the WASH-1400 fan model:

Lognormal,
Mean - 3.0E-4/d,
Error factor - 3.

Auto Flush Screen Blockage

Blockage of the auto flush filters in the diesel generator cooling is modeled by this failure mode. The GE LaSalle study has a value of 1.7E-6/hr. for filters of liquids. The IREP model is used here, with a factor of 10; the potential conservation is acknowledged:

Lognormal,
Mean - 3.0E-5/hr.,
Error factor - 10.

HPCS or Suppression Pool Strainer Blockage

An informal review of filter-related LERs indicated a 10 to 1 difference between filters and suppression pool screen failures. Thus, a value of 0.1 of the filter value is used here. It should be noted that no pump failure has been observed due to strainer blockage. But the screens have been observed to weaken and break due to corrosion. The model is:

Lognormal,
Mean - 3.0E-6/hr.,
Error factor - 10.

Water Heat Exchanger Blockage

The GE LaSalle study uses a value of 5.7E-6/hr. The model is based on the GE value with an error factor of 10:

Lognormal,
Mean - 5.7E-6/hr.,
Error factor - 10.

Fan Motor Failure to Start

The EI data survey presents a value of 3.5E-5/d. WASH-1400 has a mean value of 3.0E-4/d. The IREP and GE LaSalle studies did not model this failure mode. The WASH-1400 model for motors is used, although it may represent a conservative estimate:

Lognormal,
Mean of 3.0E-4/d,
Error factor - 10.

Fan Motor - Failure to Run

The GE LaSalle study and IREP do not have this failure mode. The EI data survey presents a value of 2.7E-5/hr. The WASH-1400 model has a similar estimate, 1.0E-5/hr. The WASH-1400 model is used here:

Lognormal,
Mean - 1.0E-5/hr.,
Error factor - 3.

Air Heat Exchanger - Rupture

This failure mode represents rupture in the heat exchangers of air coolers. The EG&G Clinch River Breeder Reactor PRA, (Reference 2) models this failure mode as:

Lognormal,
Mean - 3.0E-5/hr.,
Error factor - 10.

Fuses - Premature Opening

The EI data survey presents a value of 3.2E-8/hr., which is considerably less than values shown in WASH-1400, IREP, and the Clinch River PRA. The IREP model is used here:

Lognormal,
Mean - 3.0E-6/hr.,
Error factor - 10.

Control Circuit Failure on Demand - Dampers, MOVs, Breakers, Fan, and Pump Motors

The control circuitry is modeled similarly for these various components. The Calvert Cliffs IREP PRA has a lognormal model with a mean value of 2.5E-3/d, and an error factor of 10. This estimate is supported by the INEL LER summary of valve failures. In that study, an estimate of 8.0E-3/d was calculated for MOV failure to operate, including command or control circuit failures. Without command faults, the LER failure probability is 6.0E-3/d. This implies a contribution to the MOV failure probability of 2.0E-3/d due to control circuit failure. The Calvert Cliffs model is used here:

Lognormal,
Mean - 2.5E-3/d,
Error factor - 10.

Control Circuit - Failure to Remain Open or Closed

This component failure mode is not analyzed in any source of parameter estimates, so the component is modeled by its constituent components and appropriate failure modes.

Control circuits are modeled as a combination of three components - a contact pair and two wires. Spurious failure of a control circuit involves shorting an open contact pair or shorting 1 out of 2 wires to ground. Both failure modes are estimated in IREP - Wire shorts at 3.0E-7/hr. and shorts across open contact pairs at 3.0E-8/hr. The resulting failure rate for this component failure mode is 6.3E- 7/hr. The model used here is:

Lognormal,
Mean - 6.3E-7/hr.,
Error factor - 10.

2.6.6 Maintenance Unavailabilities

Motor Driven Pump - Maintenance Unavailability

The ORNL IPRDS analysis presents some information on maintenance related outages. In Tables 14 and 15 of that document, plant-specific values are given for pumps classified by the system. Overall numbers are not calculated. The range of values from these two tables is 1.4E-6/d to 3.0E-4/d. The presentation is somewhat vague, so the ASEP generic model is used, though it may be conservati' ' in view of the IPRDS information:

Lognormal,
Mean - 3.0E-3/d,
Error factor - 10.

Motor Driven Pump - Maintenance Unavailability Rate

The ORNL IPRDS analysis presents values for various pump maintenance failure rates. Overall estimates are not calculated. Most of the pump rates were sufficiently close to 1.0E-4/hr. to support the ASEP model as the basis for this failure mode:

Lognormal,
Mean - 1.0E-4/hr.,
Error factor - 10.

Valve Maintenance Unavailability Rate

The ORNL IPRDS analysis presents corrective maintenance frequencies for various types of valves on Table 9 of the IPRDS valve document. BWR MOVs have a higher frequency than do BWR AOVs - 2.4E-5/hr. compared to 3.9E-6/hr. The MOV rate is taken as the basis for the RMIEP model. This may be introducing a conservatism with respect to AOVs. The model used is:

Lognormal,
Mean - 2.4E-5/hr.,
Error factor - 10.

Valve Maintenance Unavailability

The IPRDS does not calculate demand-related values. The ASEP generic model is used here:

Lognormal,
Mean - 3.0E-4/d,
Error factor - 10.

Circuit Breaker (480V) Maintenance Unavailability

The only information on this failure mode is the Calvert Cliffs IREP PRA. That model is used here:

lognormal,
Mean - 1.0E-5/d,
Error factor - 5.

Air Cooler Heat Exchanger Maintenance

The model used here is from the Calvert Cliffs IREP PRA:

Lognormal,
Mean - 3.0E-4/d,
Error factor - 10.

Heat Exchanger Maintenance Failure Rate

The model used here is from Calvert Cliffs IREP PRA:

Lognormal,
Mean - 3.0E-4/hr.,
Error factor of 10.

Diesel Generator Maintenance

The AC Power Study (Reference 11) analyzed diesel generator maintenance and calculated an industry average failure probability of 6.0E-3/d. The closeness of the plant-specific estimates on page 318 of the AC Power Study suggest low uncertainty for this estimate. Even with Dresden, a noted outlier, included, 93% of all BWR plant estimates fall below 1.8E-2/d. The RMIEP model is:

Lognormal,
Mean - 6.0E-3/d,
Error factor - 3.

Fan Motor Maintenance

The Calvert Cliffs IREP PRA model for this failure mode is used here:

Lognormal,
Mean - 5.0E-4/d,
Error factor of 2.

2.6.7 Initiating Events

Internal initiating events can be grouped into three basic categories - Loss of Coolant Accidents (LOCAs), plant transients, and special transients. Special plant transients include any transient event which does not fall into categories of transient events as defined by EPRI.[22] Examples of such special initiators are - loss of service water system, loss of instrument air, and loss of a DC bus.

With one exception, the models for LOCA initiators have not changed since WASH-1400. The exception is the addition of recirculation pump seal LOCA events to the small LOCA category. The transient frequencies are subject to updating as new data becomes available. Two recent documents, References 21 and 29, were used to quantify transient initiators based on EPRI's categories. Special initiators are quantified using pertinent sources of information.

LOCA Initiators

There are three LOCA initiators defined by the size of the pipe break. These initiators are:

1) Small LOCA (Includes Seal LOCA)($\leq$0.005 ft^2 for Liquid breaks, $\leq$0.1 ft^2 for Steam breaks),

2) Medium LOCA (0.005 to 0.3 ft^2 for liquid breaks, 0.1 to 0.3 ft^2 for Steam breaks), and

3) Large LOCA ($\geq$0.3 ft^2) .

The WASH-1400 model is used for large and medium LOCAs. The small LOCA event is dominated by recirculation pump seal LOCAs. This value comes from an NRC memorandum on the issue, see Reference 36. Small LOCA initiators are modeled as lognormal, with a mean of 3.0E-2/yr., and an error factor of 3. Medium LOCA initiators are lognormal, with a mean of 3.0E-4, and an error factor of 3. Large LOCAs are modeled as lognormal, with a mean of 1.0E-4, and an error factor of 3.

Transient Initiators

Eight categories have been defined from the 37 BWR transient groups defined in Reference 22. These categories are:

1. Turbine Trip with Bypass Available
   EPRI Categories - 1,3,14-21,27,29,30,33-37;
2. Turbine Trip without Bypass
   EPRI Categories - 2,4,10,13;

3. Total Main Steam Isolation Valve Closes
   EPRI Categories - 5,6,7,9;
4. Loss of Normal Condenser Vacuum
   EPRI Category - 8;
5. Total Loss of Feedwater
   EPRI Categories - 22,24;
6. Trip of One Feedwater Condensate Pump
   EPRI Category - 23;
7. Inadvertent Opening of Safety-Relief Valve
   EPRI Category - 11; and
8. Loss of Offsite Power
   EPRI Categories - 31,32.

Values for these initiators are taken from Reference 21, wherein values for all the 37 BWR transient groups are calculated by the age of a power plant. Thus, experience which occurred in the first year of operation at a particular plant is analyzed with first year data from all BWR plants, and so on. The values used to calculate the frequencies of the eight transient categories are the total mean values of the individual transient groups in Reference 21. This total mean value incorporates information across all ages of a reactor.

Objections have been raised by GE and Commonwealth Edison that such values are conservatively biased by the high rates of plant trips often experienced in the first one to three years of plant operation. GE has advised that data from reactor year eight in Reference 21 is considered representative of the established operating practices at a BWR power plant. The transient frequencies calculated from year eight data are included on Table 2.13 to compare with the values based on overall data. It can be seen that the two sets of values compare well in most categories.

Transient category eight, Loss-of-Offsite-Power, was further evaluated by looking at Reference 29. This document is the 1986 version of an annual analysis of loss-of-offsite-power events by EPRI. This document presents frequencies based on overall reactor years and does not look at reactor age as a factor. This seems to be a reasonable approach, as many loss of offsite power transients can be independent of the experience of the plant staff (e.g., weather or grid-related events). The data in Reference 21 is analyzed three ways:

1. Overall Reactor History,
2. Three Most Recent Years, and
3. Most Recent Year.

The results, as shown on Table 2.13, show a strong agreement across all estimates of loss of offsite power frequency. As a result of the probable importance of the loss of offsite power frequency, a new method was developed for estimating the initiating event frequency and the probability of recovery of offsite power at various times after the initiating event. This method is presented in NUREG/CR-5032.[37] The method was used not only for the LaSalle analysis but also for all of the plants analyzed in the

NUREG-1150 effort.[38] The method takes the data on loss of offsite power for all plants and calculates a plant specific initiating event frequency based on the characteristics of the general population and the specific plant. A generic time to recovery curve is calculated based on three switchyard types. The result for the LaSalle plant was that the mean value for loss of offsite power was not much different than the screening estimate (0.096/yr. vs. 0.1/yr.). However, the distribution associated with this mean value and the probability of not recovering AC power within a certain time frame and its associated uncertainty distribution are available for incorporation into the accident sequence models. The data distributions used for this analysis are given in the Latin Hypercube input files presented in Volume 2 of this report.

With the exception of the loss of offsite power frequency, the transient frequencies are modeled as lognormal distributions, with error factors of 3. The variation of the mean values for the various EPRI BWR transient groups in Reference 21 tended to be low. An error factor greater than 3 would most likely be too conservative. The constrained sampling technique of the Latin Hypercube sampling routine prevents the inclusion of unrealistically large values for transient frequencies with mean values greater than one.

Special Transients

Five special initiators have been identified as applicable to LaSalle. These special initiators (numbered consecutively from the regular transients) are:

9. Loss of a 125 VDC Bus,
10. Loss of a 4160 VAC Bus,
11. Loss of Instrument Air,
12. Loss of Drywell Pneumatic, and
13. Loss of 100 lbf Drywell Pneumatic.

The loss of the DC and AC bus event models are from the ASEP data base. They are modeled:

Lognormal,
Mean - 5.0E-3/yr.,
Error factor - 3.

The other special initiator screening estimates are 50% Chi Square estimates based on no events in 275 BWR years. This event is modeled as:

Lognormal,
Mean - 3.0E-3/yr.,
Error factor - 3.

The special initiator, loss-of-drywell-pneumatic, is the same as loss-of-instrument-air.

Table 2.7
Pump Failure Rates

Screening Code	Component Failure Mode	Screening Value	Sources					RMIEP Model
1	Motor Driven Pump Demand Failure (Hardware)	3.0E-3/d	IPRDS 5.5E-3/d	WASH-1400 1.2GE-3/d EF = 3	IREP 3.0E-3/d EF = 10 GE 3.2E-4/d	LERs 4.0E-4/d	LASL FRAC 3.0E-3/d	ln,Mean = 4.0E-4/d EF = 10
2	Motor Driven Pump Failure to Run (Standby)	3.0E-5/hr.	IPRDS 2.4E-5/hr.	WASH-1400 9.0E-5/hr. EF = 10 LERs 7.0E-6/hr.	IREP 3.0E-5/hr. EF = 10	LASL FRAC 5.2E-5/d	GE 9.6E-6/hr.	ln,Mean = 3.0E-5/hr. EF = 10
3	Turbine Driven Pump Demand Failure	3.0E-2/d	IPRDS 1.1E-2/d	IREP 3.0E-2/d EF = 10	LERs 1.0E-2/d	LASL FRAC 8.0E-4/d	GE --	ln,Mean = 3.0E-2/d EF = 10
4	Turbine Driven Pump Failure to Run	1.0E-4/hr.	IPRDS 1.0E-4/hr.	IREP 1.0E-5/hr. EF = 3	LERs 6.0E-5/hr.	FB* Plant Data 5.0E-3/hr. EF = 10	GE --	ln,Mean = 5.0E-3/hr. EF = 10

*Peach Bottom, Unit 2

Table 2.8
Valve Failure Rates

Screening Code	Component Failure Mode	Screening Value	Sources				RMIEP Model
6	Moter Valves, Failure to Remain Open	1.0E-7/hr.	IPRDS 2.0E-7/hr. (PWR)	WASH-1400 1.0E-7 EF = 3	IREP (All Valves) 1.0E-7/hr. EF = 3	LERs (Command Faults Only) 6.0E-8/hr.	ln,Mean = 1.0E-7/hr. EF = 3
7	Motor Valves, Failure to Remain Closed	3.0E-7/hr.	IPRDS (Internal Leakage) 2.0E-7/hr. (PWR)	WASH-1400 3.0E-8/hr. EF = 10	IREP (All Valves) 5.0E-7/hr. EF = 100	LERs No Values	ln,Mean = 5.0E-7/hr. EF = 10
6	Air Valves, Failure to Remain Open	1.0E-7/hr.	IPRDS 7.0E-8/hr.	WASH-1400 1.0E-4/d EF = 3	IREP (All Valves) 1.0E-7/hr. EF = 3	LERs No Values	ln,Mean = 1.0E-7/hr. EF = 3
7	Air Valves, Failure to Remain Closed	3.0E-7/hr.	IPRDS (Internal Leakage) 7.0E-8/hr.	WASH-1400 3.0E-8/hr. EF = 10	IREP (All Valves) 5.0E-7/hr. EF = 100	LERs No Values	in,Mean = 5.0E-7/hr. EF = 10
6A	Check Valve, Failure to Remain Open	7.0E-7/hr.	IPRDS Defined, but not Estimated		IREP (All Valves 1.0E-7/hr. EF = 3	EI Data 1.6E-6/hr.	ln,Mean = 1.0E-7/hr. EF = 3
8	Check Valve, Failure to Operate On Demand	1.0E-4/d	LERs 8.0E-5/d		IREP 1.0E-4/d EF = 3	GE 1.0E-4/d	ln,Mean = 1.0E-4/d EF = 3

Table 2.8
Valve Failure Rates (Concluded)

Screening Code	Component Failure Mode	Screening Value	Sources				RMIEP Model
13	Motor Operated Valves Failure to Open or Close	3.0E-3/d	IPRDS 5.3E-4	WASH-1400 1.0E-3 EF = 3	IREP 3.0E-3 EF = 10	LERs 6.0E-3	LASL FRAC 7.2E-3 GE 7.8E-3	ln,Mean = 5.0E-4/d EF = 10
6	Manual Valve, Failure to Remain Open	1.0E-7/hr.	IPRDS 6.0E-8/hr.	IREP All Valves) 1.0E-7/hr. EF = 3	EI Data 2.2E-8/hr.			ln,Mean = 1.0E-7/hr. EF = 3
6	Solenoid Valve Failure to Remain Open	1.0E-7/hr.	IPRDS 7.0E-8/hr.	IREP (All Valves) 1.0E-7/hr. EF = 3	EI Data 3.0E-8/hr.			ln Mean = 1.0E-7/hr. EF = 3
17	BWR Relief Valves Failure to Reclose	3.0E-2/d	IREP 3.0E-2 EF = 10	LERs 3.0E-3	GE --	LaSalle Data 8.3E-4/d		ln,Mean = 8.3E-4/d EF = 3

Table 2.9
Electrical Component Failure Rates

Screening Code	Component Failure Mode	Screening Value	Sources							RMIEP Model
			LERs			EI Data		IREP	GE	
29	Circuit Breaker Failure to Operate	3.0E-3/d		FTO	FTC	FTO	FTC	3.0E-3/d	1.0E-6/hr.	ln,Mean = 5.0E-4/d EF = 10
			DG Output	1.4E-4/d	7.0E-4/d	3.2E-3/d	7.4E-3/d	EF = 10		
			Load	3.1E-5/d	8.8E-5/d					
			Feed	-	1.6E-7/hr.					
30	Circuit Breaker Failure to Remain Open or Closed	3.0E-5/hr.	LERs			EI Data	WASH-1400			ln,Mean = 3.0E-6/hr. EF = 10
				FTO	FTC					
			DG Output	4.5E-7/hr.	2.2E-7/hr.	2.9E-6/hr.	3.0E-6/hr.			
			Load	1.1E-7/hr.	7.7E-10/hr.	IREP	EF = 10			
			Feed	2.1E-7/hr.	6.1E-9/hr.	1.0E-5/d				
31	Diesel Generator Failure to Start	3.0E-2/d	IPRDS 3.0E-3/d	LERs Weekly Test 1.0E-2/d Monthly Test 4.0E-2/d	AC Power Study (Reference 11) 2.5E-2/d		IREP 3.0E-2/d EF = 3	GE 2.5E-2		ln,Mean = 2.5E-2/d EF = 3
32	Diesel Generator Failure to Run	3.0E-3/hr.	IPRDS 6.4E-3/hr.	AC Power Study 2.4E-3/hr.		IREP 3.0E-3/hr. EF = 10	GE 2.4E-3/hr.			ln,Mean = 2.4E-3/hr. EF = 10
139	Diesel Generator Control Circuit Failure to Start	1.0E-3	AC Power Study (Ref. 11) 2.5E-3							ln,Mean = 2.5E-3/d EF = 3

Table 2.9
Electrical Component Failure Rates (Concluded)

Screening Code	Component Failure Mode	Screening Value	Sources				RMIEP Model
140	Diesel Generator Control Circuit Failure to Run	1.0E-3/hr.	AC Power Study (Ref. 11) 2.4E-3/hr.				ln,Mean = 2.4E-3/hr. EF = 10
37,38	Relay Failure to Energize or Deenergize	3.0E-6/hr.	WASH-1400 1.0E-4/d EF = 3	IREP (Coil Failure) 3.06E-6/hr. EF = 10	GE 4.0E-7/hr.	EI Data (Spurious Operation) 1.5E-7/hr.	ln,Mean = 3.0E-6/hr. EF = 10
39	Contact Pair Failure to Open or Close	3.0E-4/d	EI Data Relay FTO or FTC 5.3E-6/d	IREP 3.0E-4/d EF = 10	GE --		ln,Mean = 3.0E-4/d EF = 10
40	Contact Pair Spurious Opening	1.0E-7/hr.	EI Data (Relay) 1.7E-6	WASH-1400 1.0E-7 EF = 3	IREP (Open Across -- Closed Contacts) 1.0E-7 EF = 3	GE	ln,Mean = 1.0E-7/hr. EF = 3
41	Contact Pair Spurious Closing	3.0E-8/hr.	EI Data 1.7E-6	WASH-1400 3.0E-8 EF = 10	IREP (Short Across Contacts) 3.0E-8 EF = 10	GE --	ln,Mean = 2.0E-8/d EF = 10
36	Transformer Fails to Deliver Power	1.0E-6/hr.		WASH-1400 1.0E-6/hr. EF = 3	IREP 1.0E-6/hr.	GE --	ln,Mean = 1.0E-6/hr. EF = 3

Table 2.10
Miscellaneous Component Failure Rates

Screening Code	Component Failure Mode	Screening Value	Sources			RMIEP Model
53	Damper Motor Fails to Operate	3.0E-3/d	IREP 3.0E-3/d EF = 10	GE --	See Fan Motor Failure to Start	ln,Mean = 3.0E-4/d EF = 3
56	Auto Flush Filter Blockage	3.0E-5/hr.	IREP 3.0E-5/hr. EF = 10	GE 1.7E-6/hr.		ln,Mean = 3.0E-5/hr. EF = 10
143	Suppression Pool, HPCS Strainer Groutes Fail Pumps	3.0E-6/hr.	Value is Assumed to be 0.1 of IREP Filter Value			ln,Mean = 3.0E-6/hr. EF = 10
57	Heat Exchanger (Water) Blockage	3.0E-6/hr.		GE 5.7E-6/hr.		ln,Mean = 5.7E-6/hr. EF = 10
73	Fan Motor Failure to Start	3.0E-4/d	EI Data 3.5E-5/d	WASH-1400 3.0E-4/d EF = 3	GE --	ln,Mean = 3.0E-4/d EF = 3
74	Fan Motor Failure to Run	1.0E-5/hr.	EI Data 2.7E-5/hr.	WASH-1400 1.0E-5/hr. EF = 3	GE --	ln,Mean = 1.0E-5/hr. EF = 3
79	Heat Exchanger (Air) Rupture	3.0E-5/hr.	EG&G Clinch River (Reference 2) 3.0E-5/hr. EF = 10	GE --		ln,Mean = 3.0E-5/hr. EF = 10
96	Fuses Premature Opening	3.0E-6/hr.	IREP 3.0E-6/hr. EF = 10	GE --	EG&G Clinch River 2.7E-6/hr.	ln,Mean = 3.0E-6/hr. EF = 10

Table 2.10
Miscellaneous Component Failure Rates (Concluded)

Screening Code	Component Failure Mode	Screening Value	Sources			RMIEP Model
114	Control Circuit Failure to Operate (Dampers, MOVs, Circuit Breakers, Fan Motors)	1.0E-3/d	Calvert Cliffs IREP PRA 2.5E-3/d EF = 10	--	GE	ln,Mean = 2.5E-3/d EF = 10
117	Control Circuit Failure to Remain Closed or Open	6.0E-7/hr.	RMIEP 1 of 2 wires or 1 Contact Pair Short			ln,Mean = 6.3E-7/hr. EF = 10

Table 2.11
Maintenance Failure Rates and Unavailabilities

Screening Code	Component Failure Mode	Screening Value	Sources	RMIEP Model
M1	Motor Driven Pump Unavailability	1.0E-3/d	IPRDS 1.4E-6/d to 3.0E-4/d ASEP 3.0E-3/d EF = 10	ln,Mean = 3.0E-3/d EF = 10
M2A	Motor Driven Pump (Non-Safety)	1.0E-4/hr.	IPRDS 1.0E-6/hr. to 8.1E-5/hr. ASEP 7.0E-5/hr. EF = 10	ln,Mean = 1.0E-4/hr. EF = 10
M4A	Valve Maintenance Failure Rate	3.0E-5/hr.	IPRDS MOVs-2.4E-5/hr. AOVs-3.9E-6/hr.	ln,Mean = 2.4E-5/hr. EF = 10
M10A	Relief Valve Maintenance	3.0E-5/hr.	Assumed Same as MOV, AOV Model	ln,Mean = 3.0E-5 EF = 10
M4	Valve Maintenance Unavailability	3.0E-4/d	ASEP 3.0E-4/d EF = 10	ln,Mean = 3.0E-4/d EF = 10
M13	Heat Exchanger Unavailability (Air Cooler)	3.0E-4/d	Calvert Cliffs IREP PRA 3.0E=4/d EF = 10	ln,Mean = 3.0E-4/d EF = 10
M9	Circuit Breaker Unavailability	6.0E-5/d	Calvert Cliffs IREP PRA 1.0E-5/d EF = 5	ln,Mean = 1.0E-5/d EF = 5
M13A	Heat Exchanger Failure Rate Water	3.0E-5/hr.	Calvert Cliffs IREP PRA 3.0E-5/hr. EF = 10	ln,Mean = 3.0E-5/hr. EF = 10

Table 2.11
Maintenance Failure Rates and Unavailabilities (Concluded)

Screening Code	Component Failure Mode	Screening Value	Sources	RMIEP Model
M5	Diesel Generator Unavailability	6.0E-3/d	AC Power Study 6.0E-3/d	ln,Mean = 6.0E-3/d EF = 3
M18	Fan Motor Unavailability	5.0E-4/d	Calvert Cliffs IREP PRA 5.0E-4 EF = 2	ln,Mean = 5.0E-4 EF = 2

Table 2.12
Initiating Event Frequencies - LOCAs

Initiating Event	Screening Value	Sources		RMIEP Model
Small-LOCA 2/yr. (0.005 ft^2 for Liquid) (0.01 ft^2 for Steam)	3.0E-2/yr.	Reference 36 2.7E-2/yr.	GE 1.2E-3/yr. (Does not Include Seal LOCA)	ln,Mean = 3.0E- EF = 3
Medium LOCA 4/yr. (0.005 to 0.3 ft^2 for liquid) (0.1 to 0.3 ft^2 for steam)	3.0E-4/yr.	WASH-1400 3.0E-4/yr. EF = 3	GE 6.7E-4/yr.	ln,Mean = 3.0E- EF = 3
Large LOCA 4/yr. (0.3 ft^2)	3.0E-4/yr.	WASH-1400 1.0E-4/yr. EF = 3	GE 2.1E-4/yr.	ln,Mean = 1.0E- EF = 3

Table 2.13
Initiating Event Frequencies - Transients

Initiating Event	Screening Value	Sources			RMIEP Model
		INEL Transient Study (Reference 9, 21)		Other	
		Total History	Year 8		
T1 Turbine Trip With Turbine Bypass	5.0/yr.	4.5	3.5	GE 1.7	ln,Mean = 4.5/yr. EF = 3
T2 Turbine Trip Without Turbine Bypass	0.5/yr.	0.52	0.50		ln,Mean = 0.52/yr. EF = 3
T3 Total MSIV Closure	0.7/yr.	0.61	0.50		ln,Mean = 0.61/yr. EF = 3
T4 Loss of Normal Condenser Vacuum	0.4/yr.	0.41	0.30		ln,Mean = 0.41/yr. EF = 3
T5 Total Loss of Feedwater	0.6/yr.	0.56	0.10		ln,Mean = 0.6/yr. EF = 3
T6 Trip of One Feedwater or Condensate Pump	0.2/yr.	0.20	0.25		ln,Mean = 0.20/yr. EF = 3
T7 Inadvertent Opening of a Safety Relief Valve	0.2/yr.	0.14	0.25		ln,Mean = 0.14/yr. EF = 3
T8 Loss of Offsite Power	0.1/yr.	0.10	0.15	NSAC-103 (Reference 9, 21) Total history 1985 1983-1985 .075 .094 .083	Mean = 0.096/yr. User Dist. (see Ref. 37).

Table 2.14
Special Transient Initiators

Initiating Event	Screening Value	Sources		RMIEP Model
T9 Loss of 125 VDC Bus	5.0E-3/yr.	NUREG-0666 (Ref. 13) 5.0E-3 EF = 3		ln,Mean = 5.0E-3/yr. EF = 3
T10 Loss of 4160 VAC Bus	5.0E-3/yr.	NUREG-0666 (Ref. 13) 5.0E-3 EF = 3		ln,Mean = 5.0E-3/yr. EF = 3
T11 Loss of Instrument Air	3.0E-3/yr.	50% Chi Square Estimate With No Events in 275 Reactor Years - 3.0E-3/yr.		ln,Mean = 3.0E-3/yr. EF = 3
T12 Loss of Drywell Pneumatic	3.0E-3/yr.	(Same as T11)		ln, Mean = 3.0E-3/yr. EF = 3
T13 Loss of 100 lbf Drywell Pneumatic	3.0E-3/yr.	50% Chi Square Estimate With No Events in 275 Reactor Years - 3.0E-3/yr.	1 AOV fails to remain closed	ln, Mean = 4.4E-3/yr.

The special initiator, loss-of-100 lbf-drywell pneumatic is modeled as one AOV fails-to-remain-closed. The mean value is - 5.0E-7/hr. x 8760 hr./yr. = 4.4E-3/yr. The error factor is 10, just as with AOV - failure-to-remain-closed on Table 2.8.

Lognormal,
Mean - 4.4E-3/yr.,
Error factor - 10.

2.7 References

1. M. T. Drouin, F. T. Harper, and A. L. Camp, "Analysis of Core DamageFrequency From Internal Events: Methodology Guidlines," NUREG/CR-4550, SAND86-2084, Vol. 1, Sandia National Laboratories, Albuquerque, NM, September 1987.

2. "Clinch River Breeder Reactor Plant Probabilistic Risk Assessment-Phase 1," EGG-EA-6162, EG&G Idaho, Inc., Idaho Falls, ID, January 1983.

3. IEEE (Institute of Electrical and Electronical Engineers), 1977, "IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear Power Generating Stations," IEEE Std 500, IEEE/John Wiley & Sons, Inc., New York, New York.

4. R. J. Borkowski, W. K. Kahl, T. L. Hebble, J. R. Fragola, and J. W. Johnson, "The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report - The Valve Component," NUREG/CR-3154, ORNL/TM-8647, Oak Ridge National Laboratory, Oak Ridge, TN, December 1983.

5. J. P. Drago, R. J. Borkowski, J. R. Fragola, and J. W. Johnson, "The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Data Report - The Pump Component," NUREG/CR-2886, ORNL/TM-8465, Oak Ridge National Laboratory, Oak Ridge, TN, December 1982.

6. D. D. Carlson, D. R. Gallup, A. M. Kolaczkowski, G. J. Kolb, and D. W. Stack, "Interim Reliability Evaluation Program Procedures Guide," NUREG/CR-2728, SAND82-1100, Sandia National Laboratories, Albuquerque, NM, January 1983.

7. C. F. Miller, W. H. Hubble, M. Trojovsky, and S. R. Brown, "Data Summaries of Licensee Event Reports of Valves at U. S. Commercial Nuclear Power Plants," NUREG/CR-1363, EGG-EA-5816, Rev. 1, EG&G Idaho, Inc, Idaho Falls, ID, October 1982.

8. M. Trojovsky, "Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants," NUREG/CR-1205, EGG-EA-5524, Rev. 1, EG&G Idaho, Inc, Idaho Falls, ID, January 1982.

9. A. J. Oswald, C. D. Gentillon, S. D. Matthews, and T. R.Meachum, "Generic Data Base for Data and Models Chapter of the National Reliability Evaluation Program (NREP)," EGG-EA-5887 Interim Report, Idaho National Engineering Laboratory, Idaho Falls, ID, June 1982.

10. U. S. Nuclear Regulatory Commission, "Reactor Safety Study - An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/014), U. S. Nuclear Regulatory Commission, Washington, DC, October 1975.

11. R. E. Battle and D. J. Campbell, "Reliability of Emergency AC Power Systems at Nuclear Power Plants," NUREG/CR-2989, ORNL/TM-8545, Oak Ridge National Laboratory, Oak Ridge, TN, July 1983.

12. W. K. Kahl and R. J. Borkowski, "The In-Plant Reliability Data Base for Nuclear Plant Components: Interim Report Diesel Generators, Batteries, Chargers and Inventors," NUREG/CR-3831, ORNL/TM-9216, Oak Ridge National Laboratory, Oak Ridge, TN, 1985.

13. P. W. Baranowsky, et. al, "A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants," NUREG-0666, U.S. Nuclear Regulatory Commission, Washington, DC, 1981.

14. A. C. Payne Jr., et al., "Interim Reliability Evaluation Program: Analysis of the Calvert Cliffs Unit 1 Nuclear Power Plant," NUREG/CR-3511, SAND83-2086, Sandia National Laboratories, Albuquerque, NM, March 1984.

15. C. L. Atwood and S. A. Steverson, "Common Cause Fault Rates for Diesel Generators," NUREG/CR-2099, EGG-EA-5359, Rev. 1, EG&G Idaho, Inc., Idaho Falls, ID, June 1982.

16. J. A. Steverson, C. L. Atwood, "Common cause Fault Rates for Valves," NUREG/CR-2770, EGG-EA-5485, EG&G Idaho, Inc., Idaho Falls, ID, February 1983.

17. C. L. Atwood, "Common Cause Fault Rates for Pumps," NUREG/CR-2098, EGG-EA-5289, EG&G Idaho, Inc., Idaho Falls, ID, February 1983.

18. J. P. Poloski and W. H. Sullivan, "Data Summaries of Licensee Event Reports of Diesel Generators at U. S. Commercial Nuclear Power Plants," NUREG/CR-1362, EGG-EA-5092, EG&G Idaho, Inc, Idaho Falls, ID, March 1980.

19. S. R. Brown, "Data Summaries of Licensee Event Reports of Protective Relays and Circuit Breakers at U. S. Commercial Nuclear Power Plants January 1, 1976 to December 31, 1983," NUREG/CR-4126 (Draft), EGG-2370, EG&G Idaho, Inc, Idaho Falls, ID, January 1985.

20. M. Trojovsky and S. R. Brown, "Data Summaries of Licensee Event Reports of Selected Instrumentation and Control Components at U. S. Commercial Nuclear Power Plants January 1, 1976 to December 31, 1983," NUREG/CR-1740, EGG-2307, Rev. 1, EG&G Idaho, Inc, Idaho Falls, ID, July 1984.

21. D. Mackowiak, C. D. Gentillion, and K. L. Smith, "Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessment," NUREG/CR-3862 Draft, Idaho National Engineering Laboratory, Idaho Falls, ID, June 1984.

22. A. S. McClymont and B. W. Poehlman, "ATWS: A Reappraisal," EPRI NP-2230, Electric Power Research Institute, Palo Alto, CA, January 1982.

23. R. B. Worrell and D. W. Stack, "A SETS User's Manual for the Fault Tree Analyst," NUREG/CR-0465, SAND77-2051, Sandia National Laboratories, Albuquerque, NM November 1978.

24. "dBase III," Ashton-Tate, Culver City, CA, 1984.

25. Pickard, Lowe and Garrick, "Classification and Analysis of Reactor Operating Experience Involving Dependent Events," EPRI NP-3967, Electric Power Research Institute, Palo Alto, CA, 1985.

26. H. F. Martz, R. J. Beckman, and C. R. McInteer, "FRAC (Failure Rate Analysis Code): A Computer Program For Analysis of Variance of Failure Rates," NUREG/CR-2434, LA-9116-MS, Los Alamos National Laboratory, Los Alamos, NM, 1982.

27. E. J. Kelly, G. M. Hemphill, and R. J. Beckman, "IPRDS FRAC Analysis For Valves, Pumps, and Electrical Components," Unpublished, Los Alamos National Laboratory, Los Alamos, NM, in NRC Public Document Room.

28. General Electric, "LaSalle County Station Probabilistic Safety Analysis," NEDO-31085, Class 1, General Electric, San Jose, CA, November 1985.

29. H. Wyckoff, "Losses of Off-Site Power at U. S. Nuclear Power Plants: Plants - All Years Through 1985," EPRI NSAC-103, Electric Power Research Institute, Palo Alto, CA, 1986.

30. S. M. Stoller Corporation, "Nuclear Power Experience," S. M. Stoller Corporation, Boulder, CO, updated monthly.

31. Energy Inc., "Data Survey and Data Base for Probabilistic Risk Assessment," published in "Brunswick Steam Electric Plant Probabilistic Risk Assessment, Appendix A.3," Carolina Power and Light Company, Raleigh, NC, April 1988.

32. S. Eide, et al.,"MONJU Probabilistic Risk Assessment," Energy Inc., Albuquerque, NM, February 1986.

33. R. L. Iman and M. J. Shortencarier, "A FORTRAN 77 Program and User's Guide for the Generation of Latin Hypercube and Random Samples for Use With Computer Models," NUREG/CR-3624, SAND83-2365, Sandia National Laboratories, Albuquerque, NM, March 1984.

34. M. Trojovsky, "Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants," NUREG/CR-1205, EG&G Idaho, Inc, Idaho Falls, ID, January 1980.

35. A. M. Kolaczkowski, et. al, "Analysis of Core Damage Trequency From Internal Events: Peach Bottom Unit 2," NUREG/CR-4550/4 of 10, Sandia National Laboratories, Albuquerque, NM, 1986.

36. Memorandum, A. C. Thadani to R. L Baer, "RRAB Preliminary Assessment of the Reactor Coolant Pump Seal Failure Problem" U.S. Nuclear Regulatory Commission, Washington, DC, December 12, 1980.

37. R. L. Iman and S. C. Hora, "Modeling Time to Recovery and Initiating Event Frequency for Loss of Off-Site Power Incidents at Nuclear Power Plants," NUREG/CR-5032, SAND87-2428, Sandia National Laboratories, Albuquerque, NM, January 1988.

38. U. S. Nuclear Regulatory Commision, "Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plants, Final Summary Report," NUREG-1150, U. S. Nuclear Regulatory Commission, Washington, DC, December 1990.

3.0 SCREENING RULES FOR THE HUMAN RELIABILITY ANALYSIS

The following List of Abbreviations and Glossary of Technical Terms are presented here for specific use in this chapter. It is recommended that one have a clear understanding of the terms before reading Chapter 3.

3.0.1 List of Abbreviations

Following is a list of abbreviations for various terms used in this chapter.

BHEP	Basic Human Error Probability
CD	Complete Dependence
CHEP	Conditional Human Error Probability
CR	Control Room
ECOM	Error of Commission
EF	Error Factor
EOM	Error of Omission
EOP	Emergency Operating Procedure
F_T	Total Failure Probability (or HEP)
HD	High Dependence
HEP	Human Error Probability
HRA	Human Reliability Analysis
HSP	Human Success Probability
INPO	Institute for Nuclear Power Operations
JHEP	Joint Human Error Probability
MOV	Motor-Operated Valve
NPP	Nuclear Power Plant
P&ID	Piping and Instrumentation Diagram
PC	Post-Calibration
PM	Post-Maintenance
PRA	Probabilistic Risk Assessment
PSF	Performance Shaping Factor
RF	Recovery Factor
RMIEP	Risk Methods Integration and Evaluation Program
SBLC	Standby Liquid Control
SLCS	Standby Liquid Control System
SNL	Sandia National Laboratories
T&M	Test and Maintenance
T_a	The estimated time needed to get to a proper locations plus the time needed to perform required actions once a diagnosis of an abnormal event has been made.
T_d	$T_m - T_a$, or the estimated allowable time for a correct diagnosis which still permits the performance of the required actions within the total allowable time, T_m.
T_m	The estimated maximum allowable time to have completed the necessary human actions following annunciation of an abnormal event (T_0).
T_0	The annunciation (or other compelling signal) of an abnormal event.
THERP	Technique for Human Error Rate Prediction
UCB	Uncertainty Bound
ZD	Zero Dependence

3.0.2 Glossary of Technical Terms

Following are definitions of various terms in this chapter. Any underlined term in a definition is also defined in this glossary. For definitions of other HRA-related terms, see the glossary in NUREG/CR-1278.[1]

abnormal event (condition or situation) - events that disrupt the normal conditions in a plant; in the context of this chapter, the occurrence of an initiating event, a loss-of-coolant accident, or system failures subsequent to the first two classes of abnormal events.

action - carrying out one or more activities (e.g., steps or tasks) indicated by diagnosis, operating rules, or written or memorized procedures.

activity - a general term referring to any kind of human performance, ranging from a simple motor action (e.g., flipping a toggle switch) to more complex behavior such as deciding which of two alternative courses of action to pursue. The complete sequence of activities in a pre-accident or post-accident situation includes: perceive, discriminate, interpret, diagnose, decision-making, and action. Depending on the level of familiarity and skill involved, estimated human error probabilities for one or more of the intermediate activities between perceive and action may be assessed as negligible in a human reliability analysis.

administrative control - a general term referring to the kinds of checking of human performance mandated in a plant and the extent to which plant policies are carried out and monitored, including the use of tagging systems and associated inventory systems to ensure that safety-related systems or components are restored to their normal states after completion of maintenance, calibration, or testing.

annunciator (ANN) - a short term for an annunciated display, a legend indicator with an auditory alarm to announce that a change of state has occurred.

arousal - see facilitative stress.

basic conditions - in the context of this chapter, basic conditions refer to the absence of recovery factors for human errors.

basic human error probability (BHEP) - the probability of a human error on a task that is considered as an isolated entity, i.e., not influenced by previous tasks.

between-person dependence - Dependence of one person's behavior on the behavior of another.

checker - one who is assigned to verify the accuracy of another's work, either while that person is doing the work or after its completion. The use of a checker is an example of human redundancy. A checker is not the same as the person who performs an inspection. The checker is "person oriented" whereas the inspector is "equipment oriented."

coarse screening analysis - a screening analysis that employs very general screening rules, with little basis, if any, on a plant-specific task analysis, and which may result in unduly conservative estimates of human error probabilities and response times so that very little screening (i.e., elimination) of human events is done in the systems analysis. The opposite of fine screening analysis.

common-cause failure - a failure which has the potential to fail more than one safety function and to possibly cause an initiating event or other abnormal event simultaneously, e.g., a human error that could result in miscalibration of several setpoints.

compelling signal - some kind of signal to the operator that is as demanding of attention as an annunciator.

complete dependence (CD) - (dependence between two activities performed by the same person or between activities performed by two people) - a situation in which, if the relationship between the activities or people is positive (i.e., if there is positive dependence), failure to perform one activity correctly will result in certain failure to perform the other. Similarly, if success occurs in performing the first activity, success will occur on the other. The opposite results will occur if the relationship between the activities or people is negative (i.e., if there is negative dependence).

conservative screening analysis - a screening analysis which is judged to be sufficiently conservative but not so conservative that the screening would eliminate only a few human error terms in the human reliability analysis from further consideration in the systems analysis. An ultra-conservative screening analysis may have the latter undesired result.

critical action - in the context of this chapter, a critical action is one identified in the initial systems analysis as having the potential for putting some system or component at risk, e.g., the failure to restore an important blocking valve to its normally open condition following maintenance.

critical parameters - in the context of this chapter, the critical variables pertaining to protection of the reactor core that control room operators are trained to monitor and initially respond to in the event of an initiating event, loss-of-coolant

accident, or abnormal event. Typically, the immediate emergency actions that operators are required to memorize include the state of critical parameters.

decision-making - (1) decision-making as a part of diagnosis: the act of choosing among alternative diagnoses, e.g., to settle on the most probable cause of the pattern of stimuli associated with an abnormal event; (2) post-diagnosis decision-making: the act of choosing which actions to carry out after a diagnosis has been made; in most cases, these actions are prescribed by rules or procedures, and decision-making is not required.

dependence (between two activities) - the situation in which the probability of failure (or success) on one activity is different depending on whether a success or failure occurred on the other activity. The activities may be performed by the same person (within person dependence) or different persons (between person dependence). For the same pair of activities, the level of dependence may differ for errors of commission and errors of omission.

diagnosis - the attribution of the most likely cause(s) of an abnormal event to the level required to identify those systems or components whose status can be changed to reduce or eliminate the problem; diagnosis includes interpretation and (when necessary) decision-making. This definition of diagnosis does not mean it is necessary to assign the proper name of the abnormal event in order to figure out what to do to cope with the event. The requirement for diagnosis in a post-accident situation can be minimized to the extent that the displays and emergency operating procedures clearly and unambiguously define the sequence of actions that are required after the initiation of some abnormal event.

discriminate - distinguishing one signal (or a set of signals) from another, e.g., "the coolant level in Tank A is 37 feet," or, if there are limit marks on the meter, "the coolant level is out of limits" (in the latter case, some interpretation is done for the operator by the design of the display).

disruptive stress - the bodily or mental tension resulting from the response to a stressor that threatens, frightens, worries, or angers a person, or increases that person's uncertainty, so that usually tasks are performed at a decreased level of effectiveness or efficiency.

dynamic task - one that requires a higher degree of interaction between the people and the equipment in a system than is required by routine, procedurally guided tasks. Dynamic tasks may include decision-making, keeping track of several functions, controlling several functions, or any combination of these. A post-accident

task may be classified as a dynamic task if the written emergency operating procedure is so poorly written that it is difficult to follow with ease. The operator's tasks in coping with an abnormal event may be classified either as dynamic or step-by-step tasks. Pre-accident tasks are usually classified as step-by-step tasks, e.g., restoration of valves (to their normal operating states) after maintenance.

emergency operating procedure (EOP) - special written procedures to assist operating personnel in responding to abnormal events. EOPs may be symptom-oriented or event-based.

end-failure term - the probability of reaching the terminal point in a failure path through an HRA event tree. Contributes to total-failure term.

error - see human error.

error factor (EF) - the square root of the ratio of the upper to the lower uncertainty bound, the latter term as defined herein.

error of commission (ECOM) - incorrect performance of a system-required task or action, given that a task or action is attempted, or the performance of some extraneous task or action that is not required by the system and which has the potential for contributing to some system-defined failure.

error of omission (EOM) - failure to initiate performance of a system-required task or action.

event-based emergency operating procedure - emergency operating procedures keyed to events or systems associated with abnormal conditions rather than to the related symptoms or functions. Synonym: "system-oriented EOP." The intent of these EOPs is that the operator will diagnose the specific event causing the abnormal event or accident in order to mitigate the consequences of that situation. Opposite to symptom-oriented EOP.

event tree - a graphic representation of system events in which the events are designated by limbs in the tree, and the sequence moves forward in time. The event tree is an inductive model, whereas the fault tree is a deductive model. There are several forms of event trees; the event trees in this appendix (and in NUREG/CR-1278)[1] are HRA event trees.

extraneous task or action - the performance of some activity not required by the system and which has the potential for contributing to some system-defined failure. An extraneous action may occur despite an operator's correct diagnosis because he made a simple manipulation or selection error, or an extraneous action or series of such actions may occur because of an incorrect diagnosis.

extremely high stress level - a level of disruptive stress in which the performance of most people will deteriorate drastically. This is likely to occur when the onset of the stressor is sudden and the stressing situation persists for long periods. This level of high stress is associated with the feeling of threat to one's physical well-being or to one's self-esteem or professional status, and is considered to be qualitatively different from lesser degrees of high stress. The occasion of a large loss-of-coolant accident is assessed as resulting in extremely high stress to operating personnel, as are some occasions in which more than two primary safety systems fail to function. Extremely high stress levels can be avoided by considerable practice on potential abnormal events so that the tasks can be classified as rule-based actions or skill-based actions. Synonym: "threat stress."

facilitative stress - the bodily or mental tension resulting from the internal response to a stressor that alerts a person, prods him or her to action, thrills a person, or makes him or her eager, so that usually the person performs at an optimal level of effectiveness or efficiency.

failure path - any path through an HRA event tree that leads to an end-failure term. A failure path may have both success limbs and failure limbs.

fault tree - a graphic representation of system events starting with some deviant condition and working backwards in time. The fault tree is a deductive model, whereas the event tree is an inductive model.

fine screening analysis - a screening analysis with the following primary characteristics: (1) it is based on an initial plant-specific task analysis, (2) it includes some credit for recovery factors for human errors, and (3) it takes into account certain possibilities of dependence among tasks which could result in common-cause failures resulting from within-person or between-person dependence. A fine level of screening analysis should provide more screening than a coarse screening analysis, but should still be capable of being judged to constitute a conservative screening analysis.

function-oriented emergency operating procedure - see symptom-oriented emergency operating procedure.

general area - see: same general area.

high dependence (HD) - a level of dependence that is approximately midway between zero dependence and complete dependence on the continuum of positive dependence.

HRA event tree - an event tree representing a graphic form of task analysis in which the limbs designate human and other events as well as different conditions or influences upon these events. Success is designated by a left limb in a branching and failure is designated by a right limb. Small letters are used to label success limbs and capital letters are used to label failure limbs. The values assigned to all tree limbs (except those in the first branching) are conditional probabilities. The first limbs may also be conditional probabilities if they represent a carryover from some other tree. In any branching in the tree, the sum of the limbs is 1.0. The HRA event tree is drawn as a binary tree, i.e., only two limbs to each branching. Continuous variables are represented by one or more binary branchings. Synonyms: "probability tree diagram" and "THERP tree."

human error - any member of a set of human actions or activities that exceeds some limit of acceptability, i.e., an out-of- tolerance action where the limits of human performance are defined by the system. Synonym: "error."

human error probability (HEP) - the probability that an error will occur when a given task or activity is performed. Synonyms: "human failure probability" and "task failure probability."

human failure probability - see human error probability.

human success probability (HSP) - the complement of human error probability, i.e., 1 - HEP.

human redundancy - the use of a person to check another's work or to duplicate the work. Synonym: checker. This term is the analog of equipment redundancy in a parallel system, i.e., at least two humans must err in order for human error to contribute to the probability of some unwanted system condition.

human reliability - the probability of successful performance of the human activities necessary for either a reliable or an available system, specifically, the probability that a system-required human action, task, or job will be completed successfully within a required time period, as well as the probability that no extraneous tasks or actions detrimental to system reliability or availability will be performed.

human reliability analysis (HRA) - a method by which human reliability is estimated. In this chapter, the HRA approach described in NUREG/CR-1278[1] is used, which is sometimes called "THERP/Handbook." See - Technique for Human Error Rate Prediction.

immediate emergency actions - those actions which must be taken quickly following an abnormal event, and which are supposed to be

committed to memory by the operating personnel. See also skill-based actions.

independence (between two activities) - see zero dependence.

initiating event - abnormal events that require the plant to trip.

inspection - the recovery factor when someone looks at items of equipment to ascertain their status. If the task is to check someone else's work, the job is designated as that of a checker. The inspector is "equipment oriented" whereas the checker is "person oriented."

interpret (interpretation) - the assignment of a meaning to the pattern of signals (or stimuli) that was discriminated, e.g., "the coolant level in Task A is low, which means that the makeup pump is not running, or there is a leak somewhere, or the indicator is out of order"; if there is only one possible cause for the observed signal, the interpretation is equivalent to diagnosis.

knowledge-based actions (or behavior) - behavior that requires one to plan one's actions based on an analysis of the functional and physical properties of a system.

loss-of-coolant accident (LOCA) - a loss of reactor vessel coolant resulting from some defect such as a pipe break or leaky valve.

low dependence (LD) - a level of dependence that is greater than zero dependence but not very far up on the continuum of positive dependence.

lower (uncertainty) bound (LB) - the value of an uncertainty bound that is conservatively judged to correspond to the lower 5th percentile of human error probabilities on a lognormal scale of nominal HEPs.

misdiagnosis - an incorrect diagnosis of an abnormal event.

moderate dependence (MD) optimum conditions - a level of positive dependence between low dependence and high dependence.

moderately high stress level - a level of disruptive stress that will result in a moderate deterioration in performance effectiveness of system-required behavior for most people. The onset of an abnormal event indicated by annunciators or other compelling signals is usually classified as resulting in at least a moderately high stress level. Synonym: "heavy task load."

negative dependence - the situation in which failure to correctly perform an activity reduces the probability of failure in performing another activity, or in which success in performing an activity

reduces the probability of success in performing another activity. In the HRA Screening Rules for RMIEP, negative dependence is not employed, as it would usually lead to optimistic estimates of HEPs. Instead zero dependence is assessed.

nominal analysis - the regular probabilistic risk assessment in which the best (i.e., most accurate) estimates of failure probabilities are employed, as distinguished from the conservative (i.e., deliberately high) estimates used in a screening analysis. This chapter deals with a screening HRA as opposed to a nominal HRA.

nominal HRA - a human reliability analysis in which nominal analysis is employed.

operations personnel - personnel, usually licensed and unlicensed reactor operators, who are responsible for the daily operation of a plant.

optimum conditions - in the context of this chapter, optimum conditions refer to the presence of recovery factors for human errors. Opposite of basic conditions.

optimum stress level - the level of stress that is conducive to optimal performance.

parallel system - in the context of this chapter, a parallel system is one in which the system fails only if all of the human actions in a set are performed incorrectly and, if at least one of the incorrect actions is not corrected by successful employment of a recovery factor. For example, in a system having two locally operated valves which are on redundant paths, an operator could cause some critical system safety function to be unavailable by forgetting to restore at least one of them to the normal state following completion of maintenance. Opposite of series system.

perceive (perception) - in the context of this chapter, used in the very narrow sense of "awareness" without the further meaning of "understanding," e.g., "some annunciator tiles over there are blinking."

performance shaping factor (PSF) - any factor that influences human behavior. PSFs may be external to the operator or may be part of his or her internal characteristics.

plant policy - the operating requirements that plant management expects to be followed. Usually they are described in a formal set of written instructions that are available to all plant personnel. In some cases, they are not written but understood, e.g., the correct method of using a written check-list is to read one checklist item, perform the action required, and then read the next checklist item, and so on.

positive dependence - the situation in which failure to correctly perform a first activity increases the probability of failure in performing the second activity, and success in performing the first activity increases the probability of success in performing the second activity. In the RMIEP HRA Screening Rules in this chapter, only positive dependence is employed.

post-accident task - all tasks required to cope with an abnormal event. Post-accident tasks are divided into diagnosis and post-diagnosis actions.

post-calibration test - a test to see that some component has been properly calibrated.

post-diagnosis actions - those actions that are to be carried out once a diagnosis of an abnormal event has been made.

post-maintenance test - a test to see that some component works properly after maintenance.

pre-accident task - a term denoting activities done under normal operating conditions, including special conditions such as start up operations, or other activities that can affect the availability of equipment needed to cope with an abnormal event.

probability tree diagram - see HRA event tree.

recovery analysis - a term used by systems analysts to describe in probabilistic terms the ability of a system (including its operators) to "recover" from (i.e., cope successfully with) some abnormal event. Recovery analysis should not be confused with recovery factors.

recovery factor (RF) - a factor that prevents or limits the undesirable consequences of a human error. One of the most common RFs is human redundancy. Other RFs are the effects of displays of component status in the control room (especially those which are annunciated), the effects of post-maintenance tests or post-calibration tests, and the effects of daily checks or walk-around inspections, especially those involving the use of written checklists.

response time - the time required to perform some critical action, including travel time.

restore or restoration task - the returning of valves, circuit breakers, and other components to their normal state after completion of maintenance, calibration, or testing. Restoration is not usually considered to be part of maintenance because operations personnel rather than maintenance personnel perform the restoration tasks.

rule-based actions (or behavior) - behavior in which a person follows remembered or written rules, e.g., performance of written post-diagnosis actions or calibrating an instrument or using a checklist to restore manual valves to their normal operating status after maintenance. Rule-based tasks are usually classified as step-by-step tasks unless the operator has to continually divide his or her attention among several such tasks without specific written cues each time he or she should shift attention to a different task. In the latter case in which there is considerable reliance on memory, the overall combination may be classified as a dynamic task, especially in a post-accident situation.

same general area - in the context of this chapter, two components are in the same general area if they are no farther apart than a few steps. See same visual frame of reference.

same visual frame of reference - in the context of this chapter, two components are in the same visual frame of reference when they are in the same general area and the operator can see one of them without moving his or her head while performing some action on the other.

screening analysis - involves the use of conservative estimates of human behavior (i.e., higher human error probabilities and longer response times than one expects to be the case) to each system event or human task as an initial type of sensitivity analysis. If a screening failure probability does not have a material effect in the systems analysis, it may be dropped from further consideration.

screening HRA - a human reliability analysis in which screening analysis is employed.

sensitivity analysis - an analysis in which one or more estimates of various parameters are varied to observe their effects on a system or some part of it (e.g., in a human reliability analysis, estimates of human error probabilities would be varied to ascertain their effects in a systems analysis).

series system - in the context of this chapter, a system that will fail (or be designated as a failure) if any of the human activities in a set is performed incorrectly and not corrected by successful employment of a recovery factor. Opposite of parallel system.

skill-based actions (or behavior) - the performance of more or less subconscious routines governed by stored patterns of behavior, e.g., the performance of memorized immediate emergency actions following a loss-of-coolant accident or an initiating event, or the use of a hand tool by a person experienced with the tool. The distinction between skill-based actions and rule-based

actions is often arbitrary, but is primarily in terms of the amount of conscious effort involved, in layman terms, the amount of "thinking" required.

step - an arbitrary division of a task or subtask that usually includes the following: some type of information presented to the operator, some degree of operator processing of the information, and some type of required response. A step may or may not be part of a detailed written procedure.

step-by-step task - a routine, procedurally guided set of steps performed one step at a time without a requirement to divide one's attention between the task in question and other tasks. With high levels of skill and practice, a step-by-step task may be performed reliably without recourse to written procedures, e.g., repairing a faucet or the sequential performance of memorized immediate emergency actions. However, in such cases, the likelihood of errors of omission is increased. Pre-accident tasks or post-accident tasks may be classified as step-by-step tasks. See definitions for dynamic tasks, rule-based behavior, and skill-based actions.

stress - bodily or mental tension, ranging from a minimal state of arousal to a feeling of threat to one's well-being requiring action. Stress is the human response to a stressor. The effects of stress on human performance are curvilinear (i.e., non-monotonic), ranging from less than optimum performance when there is a lack of sufficient arousal, through optimum performance with an optimum stress level, to extremely poor or disorganized performance at the extremely high stress level.

stressor - any external or internal forces that cause bodily or mental tension (i.e., stress).

subtask - a division of a task. The distinction between a task and a subtask is arbitrary and is used for convenience only.

symptom-oriented emergency operating procedures - emergency operating procedures keyed to symptoms resulting from an abnormal event. Synonym: function-oriented EOP. The intent of these EOPs is to enable the control room personnel to verify and maintain critical parameters without having to assign a name to the abnormal event in question.

systems analysis - begins with the identification of initiating events, loss-of-coolant accidents, or other abnormal events and the determination of the related accident sequences, which are the combinations of system successes and failures that lead to core melt following an abnormal event. The systems are analyzed, and the contribution to failure is determined and quantified to provide accident sequence frequencies.

system-oriented emergency operating procedures - see event-based emergency operating procedure.

tagging system - all those administrative controls that ensure (1) awareness of any valves or other items of equipment that are in a non-normal state and (2) prompt restoration of this equipment to the normal state after the completion of test, calibration, or maintenance operations. A tagging system includes the use of tags, chains, locks, and keys, and, in addition, logs, suspense forms, computer programs and printouts, and any other techniques that provide an inventory of the above items.

talk-through - a task analysis method in which an operator describes the activities required in a task, explains what he or she is doing and the related mental processes during each activity in actual or simulated performance of a task. If the operating performance is simulated, the operator merely touches the manual controls that would be operated in a real situation and describes the control manipulation required. The operator points to displays and states what readings would be expected, while describing any expected time delays and feedback signals and the implications to the plant function of operator activities. Synonym: walk-through.

task - a level of job behavior that describes the performance of a meaningful job function; any unit of behavior that contributes to the accomplishment of some system goal or function. Usually a task is considered to consist of steps and occasionally is broken down into subtasks.

task analysis - an analytical process for determining the specific behaviors required of the human components in a system. It involves determining the detailed performance required of people and equipment and the effects of environmental conditions, malfunctions, and other unexpected events on both. Within each task to be performed by people, behavioral steps are analyzed in terms of (1) the sensory signals and related perceptions, (2) information processing, decision-making, memory storage, and other mental processes, and (3) the required responses. The level of detail in a task analysis should match the requirements for the level of human reliability analysis of interest. A screening analysis requires considerably less task analysis than a nominal analysis.

task failure probability - see human error probability.

Technique for Human Error Rate Prediction (THERP) - a method for human reliability analysis used to assess quantitatively the influence of human errors on the reliability or safety of a system. The method uses a schematic representation or abstraction of human events and related system events and their interactions. When

conditional probability values are assigned to the limbs in the HRA event trees used in THERP, mathematical estimates of the probabilities of achieving (or not achieving) certain combinations of events in the system may be obtained. THERP can accept data or estimates from any source.

THERP tree - see HRA event tree.

total-failure term (or probability) (F_T) - the sum of all the failure paths through an HRA event tree.

travel time - measured or estimated time to get from one location to another in the performance of required system actions by operating personnel or their designates. Travel time is included in measures or estimates of response time.

ultra-conservative screening analysis - in the context of this chapter, a screening analysis which makes use of the upper uncertainty bounds of total-failure terms rather than the nominal F_Ts.

uncertainty - as used in this chapter (and in NUREG/CR-1278),[1] uncertainty includes random variability in some parameter or measurable quantity and an imprecision in the analyst's knowledge about models, their parameters, or their predictions.

uncertainty bounds (UCBs) - the upper and lower bounds of human error probabilities that reflect the uncertainty in the estimation of an HEP. The UCBs include the variability of people and conditions and the uncertainty of the analyst in assigning HEPs to a task or activities in a task. The UCBs around the nominal HEPs in NUREG/CR-1278[1] are judged by the authors of that document to include at least the middle 90% of the HEPs for that task. For conservatism, these UCBs may be assessed as representing the middle 90% range of the true, nominal HEPs. (See definitions of lower bounds and upper bounds.) Uncertainty bounds are not the same as statistical confidence limits which are based on experiments.

upper (uncertainty) bound (UB) - the value in an uncertainty bound that is judged to correspond to the 95th percentile of human error probabilities in a lognormal scale of nominal HEPs.

visual frame of reference (see: same visual frame of reference).

walk-through - see talk-through.

within-person dependence - dependence of the performance of one activity performed by a person upon the performance of another activity performed by the same person.

zero dependence (ZD) (between two activities) - the kind of dependence in which the probability of failure or success on one activity is the same regardless of whether failure or success occurred on the other. The activities may be performed by the same or different persons. Synonym: "independence."

3.1 Background

This chapter (including Appendix A) presents the major part of the screening rules developed by Sandia National Laboratories (SNL) for the human reliability analysis (HRA) performed as part of the probabilistic risk assessment (PRA) for the Risk Methods Integration and Evaluation Program (RMIEP). The special HRA screening rules were developed for the screening PRA. This chapter is a slightly revised version of a "Fifth Review Draft, Appendix H - Screening Rules for the Human Reliability Analysis of the Risk Methods Integration and Evaluation Program, June 20, 1985" (Swain, 1985, internal document). It was this draft version that was applied in the RMIEP PRA. The revisions consist primarily of corrections of typos and other errors and some updating of the definitions in the glossary in response to peer review comments.

These RMIEP HRA screening rules served as the starting point for the new HRA procedure developed for the Accident Sequence Evaluation Program (ASEP), in which there is a screening and nominal procedure for both pre-accident and post-accident tasks. The new procedure is known as the ASEP HRA Procedure (NUREG/CR-4772).[2]

Appendix A of this report provides some background information for both the RMIEP HRA Screening Procedure and the ASEP HRA Procedure.

The RMIEP HRA screening rules in this chapter were developed to provide human error probabilities (HEPs) for (1) pre-accident tasks (also called test and maintenance (T&M) tasks) and for (2) post-accident tasks which are divided into diagnosis and post-diagnosis actions. In the case of post-accident tasks, the screening rules also use (1) measured or estimated response times for post-diagnosis actions and (2) estimated HEPs on a time baseline for diagnosis tasks. The term "T&M tasks" includes all the pre-accident tasks employed in the HRA. Typically in an HRA done for a full-scale PRA, such tasks are restricted to restoration tasks (i.e., the restoring of equipment to its usual status after completion of maintenance or calibration tasks), calibration tasks, and the post-calibration or post-maintenance tasks intended to verify that calibration or maintenance operations were done correctly. These tasks are generally not done by maintenance personnel; but by operations personnel or instrumentation technicians. The HRA does not typically include the actual maintenance operations of, for example, repairing a pump, as the equipment failure rate data usually includes the contribution of errors by maintenance personnel.

As compared with a nominal PRA in which one assigns the best possible estimates of conditional failure probabilities to each system event or

human task, screening analysis involves the use of: (1) conservative failure probabilities (i.e., higher than one really expects to be the case) and, when appropriate, or (2) conservative response times (i.e., longer than one really expects to be the case). These screening probabilities and response times are assigned to each system event or human task as an initial type of sensitivity analysis. If a screening failure probability does not have a material effect in the systems analysis, it may be dropped from further consideration. That is, if no cut sets appearing in the final analysis include the event, then the event did not survive probabilistic truncation and the event will not contribute to the subsequent nominal PRA. Screening reduces to a manageable level the amount of more detailed analyses to be performed in the nominal PRA. It is necessary to make a satisfactory balance between too little and too much screening. If the screening numbers are much too high, as is likely to be the case when a coarse screening level is employed, very few events and tasks will be "screened out," and the follow-on nominal PRA may be unmanageable in terms of the resources available to perform the PRA (in fact it may be impossible to obtain the screening results at an acceptably low probability level). On the other hand, if a finer level of screening is employed, there is a risk that the screening probabilities will be so low that potentially important events and tasks will be erroneously screened out, and dropped from further consideration in the subsequent detailed analyses. This consideration is not likely to affect pre-accident tasks as much as post-accident tasks since the factors affecting the pre-accident task analysis and quantification are much better understood.

This chapter, restricted to a screening HRA and directed primarily to pre-accident tasks with only limited post-accident considerations, presents our attempts to achieve this balance. A new methodology was developed as part of this program and used to perform the final definition and quantification of post-accident HRAs.[3,4] The definition and application of post-accident HRAs as part of the recovery analysis is described in Volume 3 of this report. The HRA screening rules are presented in the following sections:

3.2 Summary of the HRA Screening Procedure for Pre-Accident Tasks,
3.3 Summary of the HRA Screening Procedure for Post-Accident Tasks,
3.4 HRA Screening Rules for Pre-Accident Tasks (T&M),
3.5 HRA Screening Rules for Post-Accident Diagnosis/Misdiagnosis,
3.6 HRA Screening Rules for Post-Accident Post-Diagnosis Actions, and
3.7 References.

The special screening rules developed for RMIEP draw heavily on the HRA methodology and human performance modeling in NUREG/CR-1278 (Revised 1983).[1] If the reader is unfamiliar with any technical terms in this chapter, he should consult the glossary at the beginning of this chapter. Additional technical terms are in the glossary in NUREG/CR-1278. However, definitions of any technical terms in this chapter take precedence over the equivalent definitions in NUREG/CR-1278,[1] as in several cases, improvements have been made to definitions of terms in this chapter.

For the general relationship of HRA to PRA, see NUREG/CR-2254 (Revised 1983)[5] or EPRI NP-3583.[6] For convenience, a large number of abbreviations

are used. Consult the list of abbreviations at the beginning of this chapter for explanations.

The HRA screening rules for RMIEP represent "fine screening" as opposed to more "coarse screening." An example of the latter is on page A-8 of EPRI NP-3583,[6] in which .001, .01, and .1 are used as screening HEPs for, respectively, skill-based, rule-based, and knowledge-based actions (these latter terms are defined in Table 3.8 later in this chapter). In the present PRA, it was decided to employ a finer level of screening similar to that which was used in the Arkansas Nuclear One (ANO) Unit #1 PRA (NUREG/CR-2787).[7] Therefore, the ANO HRA screening rules were used as a starting point for the development of HRA screening rules more specific to the LaSalle plant. The basic idea behind fine screening as opposed to coarse screening is that (1) unduly conservative HEP estimates can be avoided by some, but not very much, additional human reliability analysis and (2) a sound background for the subsequent nominal HRA is framed by a fine screening approach. The fine screening analysis is more likely to identify areas in which additional HRA is needed than a coarse screening analysis.

The screening rules for the T&M tasks can be classified as a very fine level of screening. The primary characteristics of a very fine level of screening as employed in the LaSalle PRA are: (1) it is based on an initial plant-specific task analysis, (2) it includes some credit for human error recovery factors, and (3) it takes into account certain possibilities of task dependence which could result in common-cause failures resulting from within-person or between-person dependence. The screening rules for the post-accident tasks are considered to represent a less fine level of screening, and incorporate major conservatisms by assuming: (1) that any incorrect diagnosis will always be followed by a sequence leading to a reactor core melt situation and (2) that there will be insufficient time to perform any human actions outside the control room that could result in keeping the core covered. As stated above the final methodology for modeling and quantifying post-accident tasks is described in References 3 and 4 and in Volume 3 of this report.

This chapter presents that part of the screening rules developed by the HRA analyst, and does not include certain screening procedures employed by the systems analysts (with inputs from the HRA analyst) to identify the initial set of man-machine interfaces to be analyzed by the HRA analyst. The criteria used to make this identification are presented in Chapter 1 of Volume 6 of this report. Subsequent to the screening HRA, the nominal HRA was performed. A description of the nominal HRA used in the RMIEP PRA is found in Chapter 5 of Volume 3 of this report.

The screening rules in this chapter represent a step-by-step procedure which can be followed in a logical sequence. Our intent was to devise a procedure which requires a minimum of judgement, and which can be used by PRA specialists with little or no background in human performance technology. This intent does not reduce our conviction that the best HRA is done by a team of specialists including a human reliability analyst with

a strong background in human performance technology, e.g., a psychologist or human factors specialist. The screening procedure is summarized in the following two sections, 3.2 and 3.3. The procedure begins with the assumption that the man-machine interfaces to be subjected to a screening analysis have already been identified. To use the screening procedure correctly, the user must understand the background material in Sections 3.4, 3.5, and 3.6.

3.2 Summary of the HRA Screening Procedure for Pre-Accident Tasks

Tables 3.1 - 3.5 present the summary of the HRA screening procedure for pre-accident tasks. Section 3.4 provides the background material which should be studied prior to using those tables. The glossary of terms in Section 3.0 defines the technical terms which must be understood before the screening rules can be followed properly.

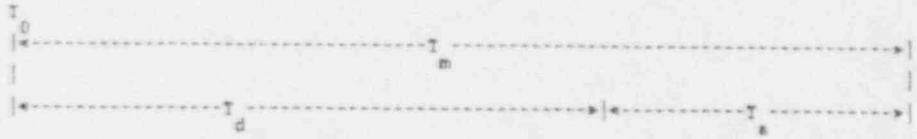
Either of two sets of estimated probabilities can be employed in the HRA screening procedure for pre-accident tasks. The first set involves the use of conservative total-failure terms (F_Ts) which have been calculated as described in Section 3.4. The second set involves the use of the upper bounds (UBs) of the estimated uncertainty bounds on the F_Ts, calculated by the application of the method for propagating uncertainty bounds in an HRA described in Appendix A of NUREG/CR-1278.[1] The use of the UBs of the F_Ts provides an ultra conservative screening procedure. Only the first set was used in the RMIEP screening analysis. Therefore, it was not necessary to calculate many of the upper bounds for application to RMIEP.

The tables list probabilities to several decimal places. As is usual in the Sandia approach to HRA, calculations are performed to several decimal places to facilitate traceability. The final answers, i.e., the F_Ts used in the system fault trees or system event trees, are rounded considerably to avoid the appearance of inappropriate exactitude.

3.3 Summary of the HRA Screening Procedure for Post-Accident Tasks

Tables 3.6 - 3.10 and Figures 3-1 and 3-2 present the summary of the HRA screening procedure for post-accident tasks. Sections 3.5 and 3.6 provide the background material which should be studied prior to using the above tables and figures.

Post-accident tasks are divided into diagnosis tasks and the post-diagnosis tasks, both of which are intended to maintain or ensure reactor protection once some abnormal event has occurred. Diagnosis refers to the probability of a correct diagnosis within the time required to permit carrying out the required post-diagnosis actions. Diagnosis is defined as attributing the most likely cause(s) of an abnormal event to the level required in order to identify those systems or components whose status can be changed to reduce



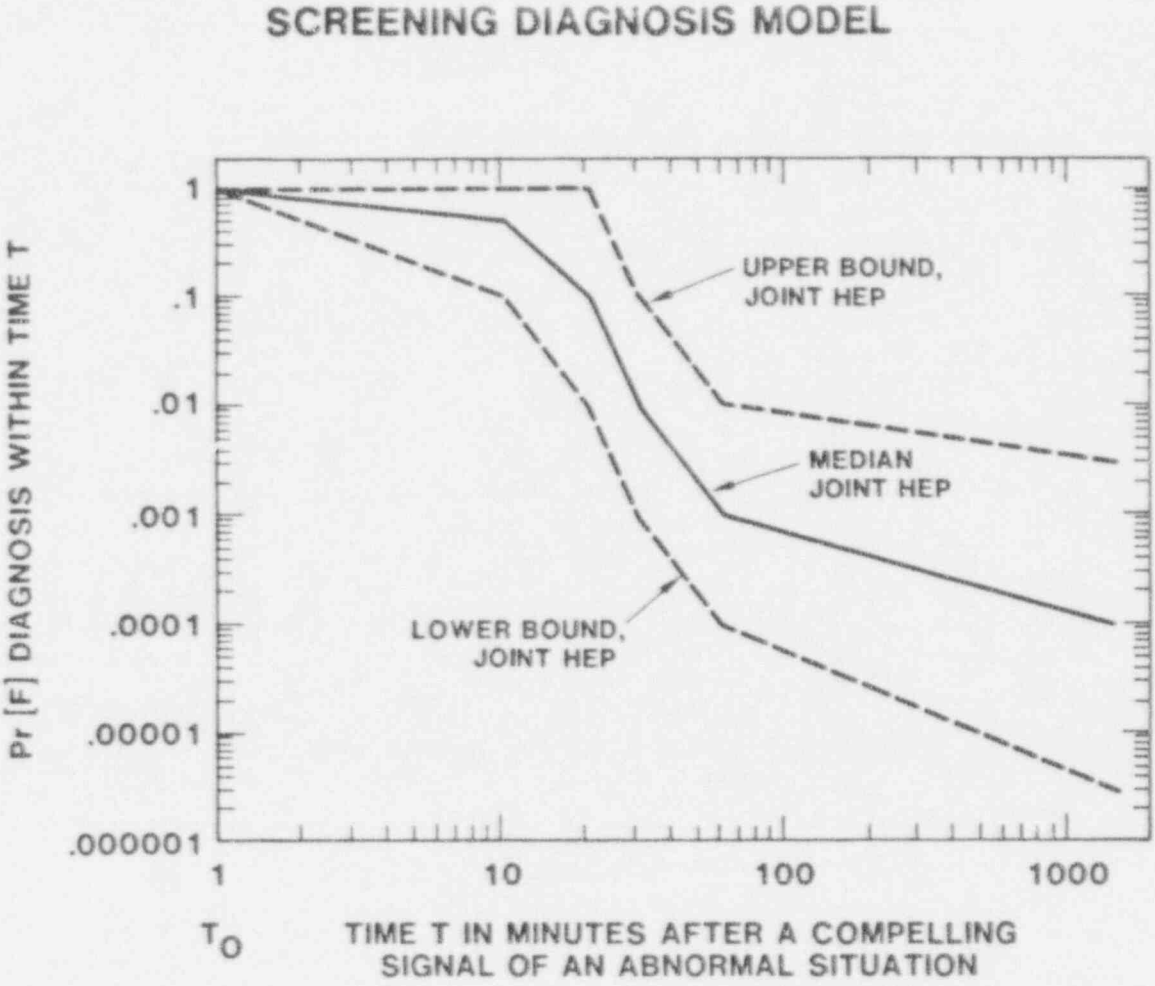
Key: T_0 - Annunciation (or other compelling signal) of an abnormal event

T_m - Estimated maximum allowable time to have correctly diagnosed the abnormal event and to have completed the required post-diagnosis actions so as to achieve system success criteria established by systems analysts

T_d - Estimated allowable time for a correct diagnosis which will still permit sufficient time to perform required post-diagnosis actions prior to T_m

T_a - Estimated time needed to get to proper locations and to perform required post-diagnosis actions after a correct diagnosis

Figure 3-1 Time Relationships Between Annunciation (or Other Compelling Signal) of an Abnormal Event, a Correct Diagnosis of the Event, and Performing the Required Post-Diagnosis Actions After a Correct Diagnosis



(Revised copy of Figure 12-3 from NUREG/CR-1278. The revision corrects the labeling of the ordinate in the figure so that the "1" occurs where the three lines in the figure meet at the ordinate, as shown in the above figure.)

Figure 3-2 Initial-Screening Model of Estimated HEPs and UCBs for Diagnosis Within Time T of One Abnormal Event by Control Room Personnel (based on Oswald et al, 1982)[8]

Table 3.1
Summary of ... Screening Procedure for Pre-Accident Tasks

1. Visit the plant initially to observe a sample of Pre-Accident tasks and obtain relevant written procedures and other documentation that spells out operating sequences and rules. Carefully evaluate the quality of the administrative control, e.g., how well prescribed pre-accident tasks, especially human error recovery factors (RFs), will be performed. (See NUREG/CR-1278[3] and -2254[5] for more detail.) Other plant visits may be necessary during the screening process, depending on how active a role plant personnel take in the HRA part of the PRA.

2. Identify the pre-accident critical actions in terms of the systems analysis. (Note: This step should be performed concurrently with Step 1.) Obtain any additional written materials required.

3. Determine for which critical pre-accident actions, errors are fully recoverable by "compelling signals," usually one or more annunciators when a maintenance or calibration task is completed or before normal power operation can be resumed.

4. Determine for which critical T&M actions, errors can be recovered by a post-maintenance (PM) or post-calibration (PC) test if the test is performed correctly.

5. Determine for which critical pre-accident actions, (1) a second person is required to directly verify component status after completion of the actions by the original performer, or (2) the original performer is required to make a separate check of component status at different time and place from his or her original performance.

6. Determine for which critical pre-accident actions there is a requirement for a shiftly or daily check of component status in or outside of the control room, using a written list. No recovery credit is given for such checks without a written list.

7. Assign a basic HEP (BHEP) of .02 for each error of omission (EOM) and .01 for each error of commission (ECOM). Assume that an ECOM is always possible if an EOM is not made. Therefore, for each critical action, assign a total BHEP of .03.

8. Assign a .1 HEP for failure of each relevant RF, except for a .01 failure to perform a required PM or PC test or to perform it correctly. The RF already includes between-person dependence, and is assumed to apply to the EOM and ECOM as a unit, i.e., to the BHEP of .03 for a complete critical action. The RF also includes estimated failures of administrative control, i.e., failure to perform the prescribed RF.

Table 3.1
Summary of the Screening Procedure for Pre-Accident Tasks (Concluded)

9. Consult Table 3.2 to ascertain which set of conditions apply to each critical action, and for the restrictions in the number of RFs to use. No other RFs are allowed other than those in Table 3.2.

10. Consult Table 3.3 to determine which of nine cases applies to each critical action. For each case, the appropriate total-failure probability (F_T) and its upper bound (UB) are listed, exclusive of the effects of within-person dependence. For a conservative screening analysis, use the F_Ts in Tables 3.3 and 3.5. For an ultra conservative screening analysis, use the UBs of the F_Ts in these tables.

11. Decide whether the critical human actions constitute a parallel or a series system.

12. For a series system, assess zero dependence (ZD) among components. To obtain required information for assessing within-person dependence in a parallel system, determine which components of interest are within the same visual frame of reference, within the same general area, or not within the same general area, and/or which operator actions are close in time (i.e., less than 2 minutes). If information on physical separation cannot be obtained, assume the components are in the same visual frame of reference. If information on time cannot be obtained, assume the actions occur closely in time.

13. Consult Table 3.4 to assess the level of dependence between the critical human actions performed by an operator which are related to the components in question. For simplicity, assume that the level of dependence in any set of related components remains constant.

14. Consult Table 3.5 to determine the F_Ts (or UBs of the F_Ts) for any of the nine cases (in Table 3.3) relevant to the analysis, as modified for multiple-component systems and for the effects of dependence (from Table 3.4).

15. Enter the F_Ts (or UBs of the F_Ts) in the appropriate system fault trees or system event trees, paying special attention that the dependence effects identified for human actions are preserved in the way in which the F_Ts are used. See Chapters 5 and 10 of NUREG/CR-1278[1] for guidelines.

Table 3.2
Basic and Optimum Conditions for HRA Screening of
Pre-Accident Tasks, Exclusive of Within-Person Dependence Effects

---

Note: "Basic Conditions" refer to the absence of error recovery factors. "Optimum Conditions" refer to the presence of error recovery factors. Each numbered Basic Condition has its same numbered complementary Optimum Condition.

Basic Conditions

1. Unavailable component status is not indicated in the control room by some "compelling signal" such as an annunciator when the maintenance or calibration task or subsequent test is finished or before normal power operations can be resumed.

2. Component status is not verified by a post-maintenance (PM) or a post-calibration (PC) test; it is not required or, if performed, does not verify component status.

3. There is no requirement for a recovery factor (RF) involving (1) a second person directly to verify component status after completion of a maintenance or calibration task or (2) the original performer to make a separate check of component status at a different time and place from his or her original task performance.

4. Shiftly or daily checks of component status (in or outside of the control room) are done without a written checkoff list, or are not done at all.

Note: If all of the above basic conditions apply (i.e., there are no recovery factors), the basic HEP of .03 is assessed, or, for an ultra-conservative screening analysis, its upper bound of .15 is assessed.

Optimum Conditions

1. Unavailable component status is indicated in the control room by some "compelling signal" such as an annunciator when the maintenance or calibration task or subsequent test is finished or before normal power operation can be resumed.

2. Component status is verifiable by a PM or PC test. If done correctly, full recovery of any related error is assumed. An HEP of .01 is assessed for failure to perform the test or to perform it correctly.

Table 3.2
Basic and Optimum Conditions for HRA Screening of
Pre-Accident Tasks, Exclusive of Within-Person Dependence Effects
(Concluded)

3. There is a requirement for an RF involving (1) a second person directly to verify component status after completion of a maintenance or calibration task, or (2) the original performer to make a separate check of component status at a different time and place from his or her original task performance. An HEP of .1 is assessed for failure of this RF to catch an error by the original task performer. This RF is presumed to be inoperative if a required PM or PC test is not performed correctly, as such failure indicates inadequate quality assurance.

4. There is a requirement for a shiftly or daily check of component status (in or outside of the control room), using a written list. An HEP of .1 is assessed for the failure of such a check to detect the unavailable status. For screening purposes, this RF may be used only once per error.

Note: If all of the above optimum conditions apply, or if optimum condition 1 only applies, a negligible HEP is assessed due to the excellence of the recovery factors. If an ultra-conservative screening analysis is being employed, use an HEP of .00001.

Table 3.3
Applications of Table 3.2, Exclusive of Within-Person Dependence Effects

---

Note 1: For each case below, the total failure probability, F_T, is listed with its error factor (EF) and upper bound (UB) in parentheses. For a conservative screening analysis, use the F_Ts; for an ultra-conservative analysis, use the UBs of the F_Ts.

Note 2: In the first 4 cases, the post-maintenance (PM) or post-calibration (PC) test is not effective in the sense that, even if performed correctly, it will not catch the original error.

Case I - PM or PC Test not effective, no other RFs used:
- a. All Basic Conditions apply.
- b. BHEP = .03 = F_T. (EF = 5, UB = .15).

Case II - PM or PC Test not effective, both other RFs used:
- a. Basic Conditions 1, 2 apply.
- b. Optimum Conditions 3, 4 apply.
- c. F_T = .03 x .1 x .1 = .0003. (EF ~ 16, UB ~ .005).

Case III - PM or PC Test not effective, second person or other immediate RF used:
- a. Basic Conditions 1, 2, 4 apply.
- b. Optimum Condition 3 applies.
- c. F_T = .03 x .1 = .003. (EF ~ 10, UB = .03).

Case IV - PM or PC Test not effective, periodic check is made:
- a. Basic Conditions 1, 2, 3 apply.
- b. Optimum Condition 4 applies.
- c. F_T = .03 x .1 = .003. (EF ~ 10, UB = .03).

Note 3: In the last 2 cases, the PM or PC Test is effective, i.e., if performed correctly it will detect the original error.

Case V - Original error is annunciated, PM or PC Test is effective if performed correctly, both other RFs used:
- a. At least Optimum Condition #1 applies.
- b. F_T = negligible. (UB = .00001).

Case VI - PM or PC Test is effective if performed correctly, no other RFs used:
- a. Basic Conditions 1, 3, 4 apply.
- b. Optimum Condition 2 applies.
- c. Probability of not performing or not performing correctly required PM or PC Test = .01
- d. F_T = .03 x .01 = .0003. (EF ~ 10, UB = .003).

Table 3.3
Applications of Table 3.2, Exclusive of Within-Person Dependence Effects (Concluded)

Case VII - PM or PC Test is effective if performed correctly, both other RFs are used:

a. Basic Condition 1 applies.
b. Optimum Conditions 2, 3, 4 apply.
c. F_T = .03 x .01 x 1.0 x .1 = .00003. (EF = 16, UB = .0005).

(Note: The 1.0 means no recovery credit is given for Optimum Condition 3 if the PM or PC Test is not done or done correctly per Optimum Condition 2.)

Case VIII - PM or PC Test is effective if performed correctly, second person or other immediate RF is used:

a. Basic Conditions 1, 4 apply.
b. Optimum Conditions 2, 3 apply.
c. F_T = .03 x .01 x 1.0 = .0003. (EF = 10, UB = .003).

Case IX - PM or PC Test is effective if performed correctly, periodic check is made:

a. Basic Conditions 1, 3 apply.
b. Optimum Conditions 2, 4 apply.
c. F_T = .03 x .01 x .1 = .00003. (EF = 16, UB = .0005).

Table 3.4
Guidelines for Assessing Within-Person Dependence
Levels for HRA Screening for Pre-Accident Tasks

SERIES SYSTEMS:

Assume ZD for both EOMs and ECOMs

PARALLEL SYSTEMS:

Errors of Omission (EOMs)

For the Group of Components in Question:

Level of Dependence	Actions Close in Time*		Located in Same: Visual Frame of Reference**		Located in Same: General Area Only		Operator Required to Write Something for Each Component	
	YES	NO	YES	NO	YES	NO	YES	NO
ZD		x	either		either		either	
	x			x	either		x	
HD	x			x	x			x
CD	x			x	irrelevant		either	

Errors of Commission (ECOMs)

Assume ZD Regardless of Conditions

* Actions are considered to be close in time if the actions required for each component in the group are separated by less than 2 minutes.

** Two components are in the same frame of reference if both are in view without head movement, as the operator is performing an action on one of them.

Table 3.5
F_Ts for Table 3.3 BHEPs, Modified for Multiple-Component Systems, Assuming Dependence Levels Determined by Using Guidelines in Table 3.4, and Including RFs

Note 1: The upper bounds (UBs) and lower bounds (LBs) are calculated by multiplying and dividing the F_Ts by the error factors (EFs) which are listed in parentheses. Scientific notation is used in this table to save space. The EFs may be calculated using Appendix A of NUREG/CR-1278,[1] or a Monte Carlo procedure.

Note 2: If ZD can be assessed for the EOMs in a parallel system, $F_T = (F_{T,one})^n$, where $F_{T,one}$ is the F_T for one component and n is the number of components in the system.

Note 3: In the first 4 cases, the PM or PC test is not effective in the sense that, even if performed correctly, it will not catch the original error.

Case # System & RFs	Number of Components	One Component	Parallel System (If ZD, see Note 2) CD	HD	Series System ZD
Case I	1	3E-2(5)			
	2		2E-2 (5)	1E-2 (6)	6E-2 (4)
	3		2E-2 (5)	5E-3 (7)	9E-2 (3)
	4		2E-2 (5)	3E-3 (7)	1.2E-1 (3)
	5		2E-2 (5)	1E-3 (8)	1.5E-1 (2)
Case II	1	3E-4(10)			
	2		2E-4 (10)	1E-4 (8)	6E-4 (5)
(I x .01)	3		2E-4 (10)	5E-5 (9)	9E-4 (4)
	4		2E-4 (10)	3E-5 (10)	1.2E-3 (4)
	5		2E-4 (11)	1E-5 (11)	1.5E-3 (3)
Case III	1	3E-3(10)			
	2		2E-3 (10)	1E-3 (11)	6E-3 (7)
(I x .1)	3		2E-3 (10)	5E-4 (12)	9E-3 (6)
	4		2E-3 (10)	3E-4 (13)	1.2E-2 (5)
	5		2E-3 (10)	1E-4 (14)	1.5E-2 (4)
Case IV	1	3E-3(10)			
	2		2E-3 (10)	1E-3 (11)	6E-3 (7)
(I x .1)	3		2E-3 (10)	5E-4 (12)	9E-3 (6)
	4		2E-3 (10)	3E-4 (13)	1.2E-2 (5)
	5		2E-3 (10)	1E-4 (14)	1.5E-2 (4)

Table 3.5
F_Ts for Table 3.3 BHEPs, Modified for Multiple-Component Systems, Assuming Dependence Levels Determined by Using Guidelines in Table 3.4, and Including RFs (Concluded)

Note 4: In the last 5 cases, the PM or PC test is effective i.e., if performed correctly, it will catch the original error.

Case # System & RFs	Number of Components	One Component	Parallel System (If ZD, see Note 2) CD	HD	Series System ZD
Case V	1 - 5	negligible	negligible		negligible
Case VI	1	3E-4(10)			
	2		2E-4 (10)	1E-4 (8)	6E-4 (5)
(I x .01)	3		2E-4 (10)	5E-5 (9)	9E-4 (4)
	4		2E-4 (10)	3E-5 (10)	1.2E-3 (4)
	5		2E-4 (10)	1E-5 (11)	1.5E-3 (3)
Case VII	1	3E-5(16)			
	2		2E-5 (16)	1E-5 (14)	6E-5 (9)
(I x .01	3		2E-5 (16)	negligible	9E-5 (7)
x .1)	4		2E-5 (16)	negligible	1.2E-4 (6)
	5		2E-5 (16)	negligible	1.5E-4 (6)
Case VIII	1	3E-4(10)			
	2		2E-4 (10)	1E-4 (8)	6E-4 (5)
(I x .01)	3		2E-4 (10)	5E-5 (9)	9E-4 (4)
	4		2E-4 (10)	3E-5 (10)	1.2E-3 (4)
	5		2E-4 (10)	1E-5 (11)	1.5E-3 (3)
Case IX	1	3E-5(16)			
	2		2E-5 (16)	1E-5 (14)	6E-5 (9)
(I x .01	3		2E-5 (16)	negligible	9E-5 (7)
x .1)	4		2E-5 (16)	negligible	1.2E-4 (6)
	5		2E-5 (16)	negligible	1.5E-4 (6)

Table 3.6
Post-Accident Screening Rules for HRA

1. Review the definitions and concepts in Table 3.7 and Figure 3-1.

2. For the following cases, assess the HEP = 1.0 for the entire HRA for the abnormal event in question; no further HRA is required:

   a. Critical actions must be performed outside of the control room.

   b. Critical skill-based or rule-based actions are not supported by available written procedures. This assessment is used even though it may be required for personnel to have memorized these actions. (See Table 3.8 for definitions.)

   c. The required instrumentation fails or the instrumentation is inaccurate (i.e., misleading).

3. Using systems analysis methods, and referring to Figure 3-1, estimate T_m, the maximum allowable time to have correctly diagnosed an abnormal event and to have completed the necessary human actions following T_0, the annunciation (or other compelling signal) of an abnormal event. For definitions of diagnosis and related terms, see Table 3.7.

4. Identify the actions required to successfully cope with the abnormal event, once a correct diagnosis has been made.

5. Using simulated measures (e.g., walk-throughs), estimate the time needed to get to a particular location to perform the required actions once a diagnosis of an abnormal event has been made.

   a. No credit is allowed for actions to be performed outside the control room, i.e., assess an HEP of 1.0 for such actions. Assign an HEP of 1.0 to the entire HRA for the abnormal event in question.

   b. For a simple control action (e.g., manipulation of one switch), assess 1 minute as the required travel and manipulation time combined. An example is activation of the manual trip button.

   c. If there is a requirement to use written procedures, i.e., the human actions to be performed cannot be assumed to be committed to memory, assess a 5 minute delay, after correct diagnosis, before the actions will be initiated.

   d. Apart from the above rules, estimate the travel time for each set of necessary post-diagnosis actions separately.

Table 3.6
Post-Accident Screening Rules for HRA (Concluded)

6. Using simulated measures (e.g., talk-throughs), estimate the time required to perform the necessary post-diagnosis actions once the correct location has been reached.

7. Sum the estimated times from Steps 5 and 6 to calculate T_s, the time needed to get to a particular location plus the time needed to perform required actions once a diagnosis of an abnormal event has been made.

8. Calculate $T_d = T_m - T_s$, which is the allowable time for a diagnosis which permits the performance of the required actions within the total allowable time, T_m.

9. Using T_d, select the appropriate HEP from Figure 3-2 or Table 3.9. This diagnosis HEP is considered the probability of misdiagnosis which will result in a core damage accident. For the case of more than one abnormal event occurring closely in time (i.e., within 10 minutes), use Table 3.9. For the diagnosis HEP for the four critical parameters listed below, use the lower bound values in Figure 3-2 or Table 3.9 if the recognition of these parameters can be classified as skill-based behavior per Table 3.8; otherwise, use the nominal values. The four critical parameters at LaSalle are:

   a. Check the reactor power level. It must not exceed 118%.
   b. Check the water level in the core. It must not be below 12.5 inches above instrument zero.
   c. Check the reactor pressure. It must not be over 1046 psi.
   d. Check the containment temperature and pressure. Temperature must not be over 110 degrees F and pressure must not be over 1.69 psi.

10. Select the appropriate HEP(s) for post-diagnosis action(s) from Table 3.10.

11. Calculate the estimated total-failure probability, F_T, by adding the diagnosis HEP (Step 9) to the HEP(s) for carrying out the required post-diagnosis action(s) (Step 10). If this calculation results in a total-failure probability greater than 1.0, use 1.0.

12. Enter the F_Ts in the appropriate system fault trees or system event trees, paying special attention that the dependence effects identified for human actions are preserved in the way the F_Ts are used. See Chapters 5 and 10 of NUREG/CR-1278[1] for guidelines.

Table 3.7
Definitions of Cognition-Related Terms and Usage in the Handbook

Table 12-1 Definitions of cognition-related terms and usage in the Handbook

Term	Dictionary Definition*	Handbook Usage
Cognition	the act or process of knowing, including both awareness and judgment	restricted to those aspects of behavior involved in diagnosis of abnormal events
Judgment	the process of forming an opinion or evaluation by discerning and comparing	not used in our models--too imprecise; used only in the context of expert estimation
Perceive	to attain awareness or understanding; to become aware through the senses	used in the very narrow sense of "awareness" without the further meaning of "understanding," e.g., "some annunciator tiles over there are blinking"
Discriminate	to mark or perceive the distinguishing or peculiar features of; to distinguish one like object from another	distinguishing one signal (or a set of signals) from another, e.g., "the coolant level in Tank A is 37 feet," or if there are limit marks on the meter, "the coolant level is out of limits" (in the latter case, some interpretation is done for the operator by the design of the display)
Interpret	to conceive in the light of individual belief, judgment, or circumstance	the assignment of a meaning to the pattern of signals (or stimuli) that was discriminated, e.g., "the coolant level in Tank A is low, which means that the make-up pump is not running, or there is a leak somewhere, or the indicator is out of order"; if there is only one possible cause for the observed signal, the interpretation is equivalent to diagnosis
Diagnosis	a statement or conclusion concerning the nature or cause of some phenomenon	the attributing of the most likely cause(s) of the abnormal event to the level required to identify those systems or components whose status can be changed to reduce or eliminate the problem; diagnosis includes interpretation and (when necessary) decision-making
Decide	to make a choice or judgment	"decision-making" used instead of "deciding"
Decision-Making		(1) decision-making as part of diagnosis: the act of choosing between alternative diagnoses, e.g., to settle on the most probable cause of the pattern of stimuli associated with an abnormal event (2) postdiagnosis decision-making: the act of choosing which actions to carry out after a diagnosis has been made; in most cases, these actions are prescribed by rules or procedures, and decision-making is not required
Action	a thing accomplished usually over a period of time, in stages, or with the possibility of repetition	carrying out one or more activities (e.g., steps or tasks) indicated by diagnosis, operating rules, or written procedures

*Webster (19[illegible] 9

Table 3.8
Definitions of Skill-Based, Rule-Based, and
Knowledge-Based Behavior*

Skill-Based Behavior: "In skill-based behavior there is a very close coupling between the sensory input and the response action. Skill-based behavior does not directly depend on the complexity of the task, but rather on the level of training and the degree of practice in performing the task. While different factors may influence the specific behavior of a particular individual, a group of highly trained operators would be expected to perform skill-based tasks expeditiously or even mechanistically with a minimum of mistakes. For rule- and knowledge-based behavior, the connection between sensory inputs and output actions is not as direct as in skill-based behavior." One primary characteristic of skill-based behavior is that no interpretation of the meaning of a display is required; the display must be completely unambiguous with regard to the required action to take. Rasmussen[10] notes that skill-based behavior consists of the performance of more or less stored patterns of behavior (e.g., manual control of fuel rod insertion and withdrawal, or operating a crane).

Rule-Based Behavior: "Rule-based behavior is governed by a set of rules or associations, which are known and followed. A major difference between the rule-based and the skill-based behaviors stems from the degree of practice. If the rules are not well practiced, the human being has to consciously recall or check each rule to be followed. Under these conditions the human response is expected to be less timely and more prone to mistakes, since additional cognitive processes must be called upon. The potential for error results from problems with memory, the lack of willingness to check each step in a procedure, and failure to perform each and every step in the procedure in the proper sequence." Rasmussen[10] uses the term rule-based behavior to denote behavior that requires a more conscious effort (than is the case for skill-based behavior) in following stored (or written) rules, e.g., calibrating an instrument.

Knowledge-Based Behavior: "When symptoms are ambiguous or complex, the state of the plant is complicated by multiple failures or unusual events, or the instruments give only an indirect reading of the state of the plant, the operator has to rely on his knowledge, and his behavior is determined by more complex cognitive processes. Rasmussen calls this knowledge-based behavior. The performance of the human being in this type of behavior depends on his knowledge of the plant and his ability to use that knowledge. This type of behavior is expected to be more prone to mistakes or misjudgements and require more time for the appropriate action to be taken." Rasmussen[10] applies the term "knowledge-based behavior" to cases in which the situation is, to some extent, unfamiliar--that is, where considerably more cognition is involved in one's deciding what to do.

---

*Quoted information from pp A-1 and A-3 of EPRI NP-3583[6].

Table 3.9

Initial-Screening Model of Estimated HEPs and EFs for Diagnosis Within Time T by Control Room Personnel of Abnormal Events Annunciated Closely in Time*

(Copy of Table 20-1 from NUREG/CR-1278 with appropriate changes to figure number)

Item	T (Minutes after T_0)**	Median joint HEP for diagnosis of a single or the first event	EF	Item	T (Minutes after T_0)**	Median joint HEP for diagnosis of the second event	EF
(1)	1	1.0	--	(7)	1	1.0	--
(2)	10	.5	5	(8)	10	1.0	--
(3)	20	.1	10	(9)	20	.5	5
(4)	30	.01	10	(10)	3	.1	10
				(11)	40	.01	10
(5)	60	.001	10				
				(12)	70	.001	10
(6)	1500 (~ 1 day)	.0001	30				
				(13)	1510	.0001	30

* "Closely in time" refers to cases in which the annunciation of the second abnormal event occurs while CR personnel are still actively engaged in diagnosing and/or planning responses to cope with the first event. This is situation-specific, but for the initial analysis, use "within 10 minutes" as a working definition of "closely in time."

Note that this model pertains to the CR crew rather than to one individual.

** For points between the times shown, use the medians and EFs from Figure 3-2 for the first event, and interpolate between the tabled values for the second event.

+ T_0 is a compelling signal of an abnormal situation and is usually taken as a pattern of annunciators. A probability of 1.0 is assumed for observing that there is some abnormal situation.

++ Assign HEP = 1.0 for the diagnosis of the third and subsequent abnormal events annunciated closely in time.

Table 3.10
HEP Screening Rules for Post-Accident Post-Diagnosis Actions

Item	HEP	Action
(1)	1.0	Perform a required action outside of the control room.
(2)	1.0	Perform a critical skill-based or rule-based action correctly when no written procedures are available. This assessment is used even though it may be required for personnel to have memorized these actions. (See Table 3.8 for definitions.)
(3)	.05	Perform a critical procedural action correctly for the case in which recovery is no longer possible at the location where the error occurred.
(4)	.01	Perform a critical procedural action correctly for the case in which recovery is still possible at the location where the error occurred, and the step is performed by one person and checked by another person.
(5)	.001	Perform the post-diagnosis immediate emergency actions for the four critical parameters listed in Table 3.6, when (a) these can be judged to have been committed to memory, (b) they can be classified as skill-based actions per Table 3.8, and (c) there is a backup written procedure.

or eliminate the problem. In the context of the new symptom-oriented emergency operating procedures, diagnosis does not necessarily require that some name be attached to the abnormal event, e.g., small loss-of-coolant accident (LOCA). For additional definitions of terms related to post-accident behavior, see Table 3.7. Misdiagnosis refers to a specific incorrect diagnosis, given that the correct diagnosis was not made within the allowable time. The glossary in Section 3.0 defines the technical terms which must be understood before the screening rules can be applied properly. Some of these terms are also defined in this section.

Following are some definitions and calculations related to post-accident response times:

T_0 = the time at which annunciation (or some other compelling signal) of an abnormal event occurs.

T_m = the maximum allowable time to have properly diagnosed the abnormal event and to have completed the necessary human actions following T_0

T_a = the time needed to get to a particular location plus the time needed to perform the required actions once a diagnosis of an abnormal event has been made.

T_d = T_m - T_a, or the allowable time for a diagnosis which permits the performance of the required actions within the total allowable time, T_m.

Figure 3-1 shows the required time relationships on an indefinite time baseline. The following sections show how to determine the appropriate times as well as the screening HEPs.

Unlike the HRA screening procedure for Pre-Accident tasks, the screening procedure for post-accident tasks does not provide upper uncertainty bounds as a basis for an ultra-conservative screening analysis. It is judged that the screening analysis presented herein is already sufficiently conservative, as discussed in Sections 3.5 and 3.6.

The tables for the post-accident screening analysis, like those for the Pre-Accident screening analysis, list probabilities to several decimal places to facilitate traceability of the screening HRA. Considerable rounding is employed for the final answer, i.e., for the F_Ts used in the system fault trees or system event trees, to avoid the appearance of inappropriate exactitude.

3.4 HRA Screening Rules for Pre-Accident Tasks

The purpose of this section is to explain the rationale behind the HRA screening procedure presented in Section 3.2. This section is divided into:

Early in the Pre-Accident Screening HRA, the HRA analyst devised two preliminary sets of HRA screening rules for the pre-accident tasks. These two sets are described in Sections 3.4.1 and 3.4.2, as they provide a background for understanding the two sets of final screening rules which were presented in Section 3.2 and further discussed in Sections 3.4.3 and 3.4.4. The two preliminary sets of screening rules were not as detailed as those finally adopted, nor did they provide simple rules for considering the effects of within-person or between-person dependence which could result in common-cause failures. Both sets of rules required that the HRA analyst perform a detailed HRA for each task, whereas the final screening rules adopted could be used by systems analysts with guidance by the HRA analyst. As stated in Section 3.1, the HRA screening rules adopted for the RMIEP HRA are classified as fine screening, to distinguish them from the more usual coarse screening rules frequently used in PRA. The case for fine screening is that by performing some, but not a great deal of, task analysis of pre-accident tasks, the screening HEPs developed are more realistic but still conservative. This approach reduces to a large extent the amount of nominal HRA required once the screening process has been completed, allows easier solving for the system and accident sequence cut sets, and represents a more reasonable approach given the maturity of PRA methodology (i.e., unreasonably conservative screening values need no longer be used given the current level of understanding of T&M errors).

Before introducing the preliminary and final sets of HRA screening rules for pre-accident tasks, it is necessary to emphasize the distinction between the systems analysts' use of the word "recovery" and the HRA analysts' use of the term "recovery factors" (RFs). The systems analysts think of recovery in terms of the ability of the system (including its operators) to "recover" from some unusual situation. They use the term, recovery analysis, to show quantitatively the extent to which the system is expected to recover from such events. In the HRA field, the term, recovery factor, is used in a different sense. The glossary defines a recovery factor as "a factor that prevents or limits the undesirable consequences of a human error." One of the most common RFs evaluated in an HRA is human redundancy, defined in the glossary as "the use of a person to check another's work or to duplicate the work." Other RFs usually evaluated are the effects of displays of component status in the control room (especially those which are annunciated), the effects of post-maintenance or post-calibration tests, and the effects of daily checks or walk-around inspections, especially those involving the use of written checklists.

3.4.1 Preliminary HRA Screening Rules for Pre-Accident Tasks

A preliminary HRA screening procedure was developed by the HRA specialist, based on the use of the upper bounds of the uncertainty bounds (UCBs) of tabled HEPs in NUREG/CR-1278[1] (Revised 1983). The procedure was as follows:

(1) Develop the HRA event trees (i.e., the event trees described in Chapter 5 of NUREG/CR-1278)[1] for initial errors and a generic error recovery factor afforded either by second operator checking, or by any special displays in the control room (CR), but not both. This generic recovery factor (RF) was designated as .1, for reasons described later.

(2) Use the upper bounds from the tables in NUREG/CR-1278[1] in place of the nominal HEPs. For example, if the nominal HEP were, say, .01, and the upper bound were .05, the .05 would be used as the screening nominal HEP.

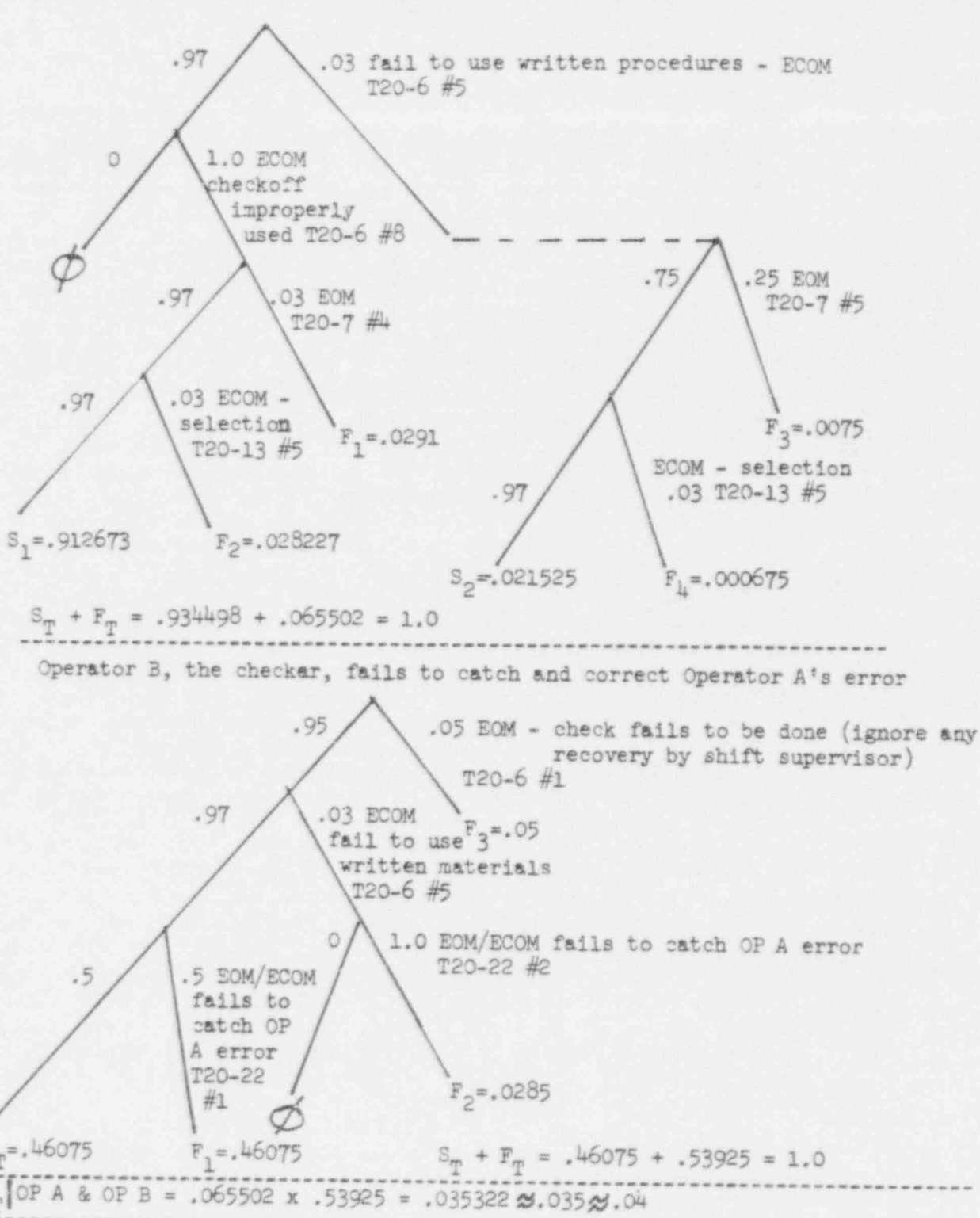
(3) Calculate the total failure probability (F_T) for each HRA event tree, including the effects of the generic error recovery factors. This value would be the screening HEP to be used by the systems analysts in their fault trees.

When the above preliminary HRA screening procedure was applied to one problem, the end results were unreasonably conservative. For example, as shown in Figure 3-3, the estimated HEP of leaving a particular manual valve open was calculated as .07 and the failure of a second operator (assigned to check the first operator's performance) to note this error was estimated as .5. Thus, the unrecovered HEP was .07 x .5 = .035, rounded to .04. In the judgement of the HRA analyst and the systems analysts, .04 constituted a highly inflated and unreasonable value for screening, and, in effect, would result in no screening at all. One could say that this type of screening represents an extreme worst case analysis because it involves multiplying worst case probabilities together.

3.4.2 Revised Preliminary HRA Screening Rules for Pre-Accident Tasks

A revised screening procedure was devised to take into account more of the plant-specific information that had been obtained by the HRA analyst and a systems analyst in the initial gross task analysis performed at the LaSalle NPP. During this task analysis, special attention was paid to the administrative control system and procedures (see Chapter 16 of NUREG/CR-1278).[1] It was important to make judgements about the probability of plant procedures being carried out as intended, and the recovery factors for errors. Following are the revised preliminary screening rules:

(1) For the primary operator error probability, use the Search Scheme from Chapter 20 in NUREG/CR-1278[1] to select the appropriate table of estimated HEPs for each failure limb in the HRA event tree.



(1) Above failure limbs use UCBs of tabled entries from NUREG/CR-1278[1]
(2) Ch. 20 Search Scheme used, assuming written procedures are correct.
(3) In Fig. A-3 of Appendix A, T20-6 #6 (test and calibration procedure is used in place of T20-6 #5 (valve restoration list), a more conservative assessment

Figure 3-3 HRA Event Trees for Preliminary HRA Screening Rules for Pre-Accident Tasks

When in doubt as to which entry in the relevant table is appropriate, use the highest nominal HEP in the table. For example, reference to Table 3.11 [Table 20-13 (T20-13) of NUREG/CR-1278][1] shows that there are five entries for possible errors in selecting locally operated valves. The HEPs for these five entries vary by an order of magnitude, from .001 for the best set of performance shaping factors (PSFs), to .01 for the worst set of PSFs. Since at the time of the HRA screening analysis, we did not have sufficient task analysis information to choose the most appropriate entry from the table, it was decided to use the largest entry, .01, as the basic HEP (BHEP). The BHEP is the probability of a human error on a task considered as an isolated entity, i.e., without regard to dependence effects.

(2) For the BHEP for the second-person verification of equipment status (e.g., after the primary operator has restored items of equipment to their operable or system-required condition, a different person visually checks each item of equipment), use the HEP of .1 from Table 3.12 (T20-22 #1 of NUREG/CR-1278,[1] i.e., Table 20-22, item #1 in the table). The .1 HEP for the failure of this RF was considered to be conservative because in most cases at the LaSalle NPP, the person performing the visual check was required to check off critical items or to write down numerical values. Also assess the .1 HEP for an RF consisting of some non-annunciated indication in the control room that was supposed to be checked soon after the performance in question. For example, the LaSalle procedures often state that following restoration procedures for a locally-operated valve, a control room indicator lamp indication of the appropriate status of the valve is to be checked and noted on a form. In many cases, following the search scheme in Chapter 20 of NUREG/CR-1278[1] would lead one to assess a much smaller HEP than .1. For conservatism, however, .1 was assessed. This .1 rule has the advantage of not requiring that a special HRA event tree be prepared for each case of an RF, as is required for the nominal HRAs. It was judged that this value would take into account those few occasions in which a required check was not carried out and this fact was not detected in the supervisor's required check of the paperwork. However, in the examples shown in Appendix A, it was not assumed that an operator would always use written procedures, as required, rather than rely on memory.

(3) Modify the above BHEPs for dependence effects according to the guidelines in Chapter 10 of NUREG/CR-1278,[1] using Table 3.13 (T20-21 of the Handbook).

(4) Prepare a table of Total-Failure HEPs (F_Ts) to be supplied to the systems analysts.

When this revised preliminary screening procedure was applied to the above example of the manual valve, the estimated HEP of leaving the valve open changed from .07 to .02, and the estimated HEP for the second person verification HEP changed from .5 to .1. Thus, the total unrecovered HEP

Table 3.11
Estimated HEPs for Selection Errors for Locally Operated Valves

Table 20-13 Estimated HEPs for selection errors for locally operated valves (from Table 14-1)

Item	Potential Errors	HEP	EF
	Making an error of selection in changing or restoring a locally operated valve when the valve to be manipulated is		
(1)	Clearly and unambiguously labeled, set apart from valves that are similar in <u>all</u> of the following: size and shape, state, and presence of tags*	.001	3
(2)	Clearly and unambiguously labeled, part of a group of two or more valves that are similar in <u>one</u> of the following: size and shape, state, or presence of tags*	.003	3
(3)	Unclearly or ambiguously labeled, set apart from valves that are similar in <u>all</u> of the following: size and shape, state, and presence of tags*	.005	3
(4)	Unclearly or ambiguously labeled, part of a group of two or more valves that are similar in <u>one</u> of the following: size and shape, state, or presence of tags*	.008	3
(5)	Unclearly or ambiguously labeled, part of a group of two or more valves that are similar in <u>all</u> of the following: size and shape, state, and presence of tags*	.01	3

*Unless otherwise specified, Level 2 tagging is presumed. If other levels of tagging are assessed, adjust the tabled HEPs according to Table 20-15.

Table 3.12
Estimated Probabilities that a Checker Will Fail to Detect Errors Made by Others*

Table 20-22 Estimated probabilities that a checker will fail to detect errors made by others* (from Table 19-1)

Item	Checking Operation	HEP	EF
(1)	Checking routine tasks, checker using written materials (includes over-the-shoulder inspections, verifying position of locally operated valves, switches, circuit breakers, connectors, etc., and checking written lists, tags, or procedures for accuracy)	.1	5
(2)	Same as above, but without written materials	.2	5
(3)	Special short-term, one-of-a-kind checking with alerting factors	.05	5
(4)	Checking that involves active participation, such as special measurements	.01	5
	Given that the position of a locally operated valve is checked (item 1 above), noticing that it is not completely opened or closed:	.5	5
(5)	Position indicator** only	.1	5
(6)	Position indicator** and a rising stem	.5	5
(7)	Neither a position indicator** nor a rising stem	.9	5
(8)	Checking by reader/checker of the task performer in a two-man team, or checking by a second checker, routine task (no credit for more than 2 checkers)	.5	5
(9)	Checking the status of equipment if that status affects one's safety when performing his tasks	.001	5
(10)	An operator checks change or restoration tasks performed by a maintainer	Above HEPs ÷ 2	5

*This table applies to cases during normal operating conditions in which a person is directed to check the work performed by others either as the work is being performed or after its completion.

**A position indicator incorporates a scale that indicates the position of the valve relative to a fully opened or fully closed position. A rising stem qualifies as a position indicator if there is a scale associated with it.

Table 3.13
Approximate CHEPs and their UCBs for Dependence Levels,* Given FAILURE on the Preceding Task

Table 20-21 Approximate CHEPs and their UCBs for dependence levels* given FAILURE on the preceding task (from Table 7-3)

Item	Levels of Dependence	BHEPs (a)	(b)	(c)
(1)	ZD**	≤ .01	.05 (EF=5)	.1 (EF=5)
		(d)	(e)	(f)
		.15 (EF=5)	.2 (EF=5)	25 (EF=5)

Item	Levels of Dependence	Nominal CHEPs and (Lower to Upper UCBs)† (a)	(b)	(c)
(2)	LD	.05 (.015 to .15)	.1 (.04 to .25)	.15 (.05 to .5)
(3)	MD	.15 (.04 to .5)	.19 (.07 to .53)	.23 (.1 to .55)
(4)	HD	.5 (.25 to 1.0)	.53 (.28 to 1.0)	.55 (.3 to 1.0)
(5)	CD	1.0 (.5 to 1.0)	1.0 (.53 to 1.0)	1.0 (.55 to 1.0)
		(d)	(e)	(f)
(2)	LD	.19 (.05 to .75)	.24 (.06 to 1.0)	.29 (.08 to 1.0)
(3)	MD	.27 (.1 to .75)	.31 (.1 to 1.0)	.36 (.13 to 1.0)
(4)	HD	.58 (.34 to 1.0)	.6 (.36 to 1.0)	.63 (.4 to 1.0)
(5)	CD	1.0 (.58 to 1.0)	1.0 (.6 to 1.0)	1.0 (.63 to 1.0)

*Values are rounded from calculations based on Appendix A. All values are based on skilled personnel (i.e., those with ≥6 months experience on the tasks being analyzed.

**ZD = BHEP. EFs for BHEPs should be based on Table 20-20.

†Linear interpolation between stated CHEPs (and UCBs) for values of BHEPs between those listed is adequate for most PRA studies.

was reduced from .035 to .002, a factor of 17.5 reduction. (These calculations are shown in Figure A-3 in Appendix A.) This reduction was not considered to be unduly optimistic as there were still additional error recovery factors not taken into account, the HEPs were based on a poorer set of PSFs than we judged to be truly the case at the LaSalle NPP, and a more conservative tabled BHEP was employed, i.e., .05 rather than .01 for the failure to use written procedures (see footnote in Figure 3-3). These judgements were based on talk-throughs of some T&M procedures at the plant.

Even with the revised preliminary screening procedure, it was quickly determined that the amount of work that would be required could not be performed within the available time and money resources. For example, Appendix A to this report shows calculations of screening HEPs for only a few human actions. If these types of analyses were attempted for all possible human errors in pre-accident tasks, the available resources for the screening analysis would be greatly exceeded. Therefore, a final HRA screening procedure was devised, as described below in Section 3.4.3.

3.4.3 Final HRA Screening Rules for Pre-Accident Tasks: Set 1

This section presents the first set of final screening rules, and Section 3.4.4 presents a more conservative, alternative version of the first set. In the RMIEP screening analysis, only the first set was used, due to time limitations.

3.4.3.1 Basic HEP for Pre-Accident Screening HRA

Based on the HRAs in Appendix A, and on a review of several other pre-accident tasks, an HEP of .02 was selected as a conservative BHEP for errors of omission (EOMs), exclusive of any recovery factors (RFs), and an HEP of .01 as the BHEP for errors of commission (ECOMs), again exclusive of RFs. These estimates, as shown in Appendix A, include what we judge to be conservative estimates of the probabilities of operators not using written procedures, as required, but instead relying on memory.

For screening purposes, we make the conservative assumption that an ECOM is always possible, provided that an EOM was not made. Thus for each critical action that must be accomplished, e.g., restoring a valve to its normal operating position after maintenance, or performing a critical step in a calibration procedure, a total BHEP of .03 is used. The .03 represents the sum of the two possible failures, either (1) an EOM or (2) no EOM but an ECOM. Algebraically, the total-failure probability for a one-component system is,

$$F_T = .02 + (.98 \times .01) = .0298 \sim .03$$

3.4.3.2 Recovery Factors for the Pre-Accident Screening HRA

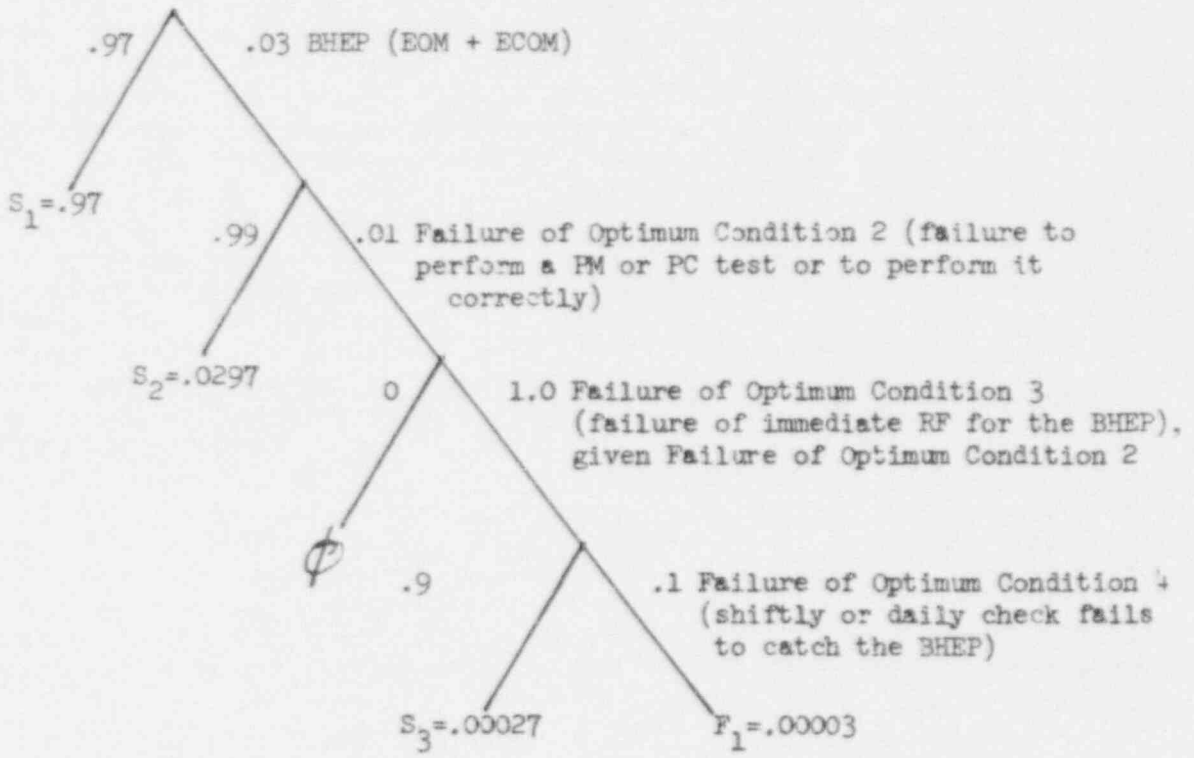
Recovery factor HEPs are designated as .1, except for a .01 HEP of failing to perform or to perform correctly a required post-maintenance test or a

post-calibration test. The .1 HEP is the nominal recovery BHEP for human redundancy stated as item #1 in Table 3.12. For screening purposes, the number of separate recovery factors is severely limited, as shown in Table 3.2 in Section 3.2. That table lists the basic conditions in which no RFs are presumed to be available, and the optimum conditions in which all allowable RFs are present. In the table, each numbered basic condition has its same numbered complementary optimum condition. For a case in which all of the basic conditions apply, the BHEP of .03 is assessed as the human-caused failure of some critical safety component or system that is unavailable. For a case in which all of the optimum conditions apply, F_T is considered to be negligible. In fact, if optimum condition #1 alone from Table 3.2 applies (i.e., unavailable component status in the CR is announced by some compelling signal), F_T is assessed as negligible. A conservative rule is shown in Item 3 under the optimum conditions listed in Table 3.2, in which the RF for an immediate check on the accuracy of a human operation is counted only once even in the case in which one check is made at the site of the operation and a different one inside the control room. Similarly, even though there may be a requirement for a shiftly or daily check of component status (optimum Item 4 in Table 3.2, for screening purposes no credit for the RF is allowed unless a written list is required for the checker, this RF is counted only once, and a .1 BHEP is assessed). These assessments represent major conservatisms. Other screening rules for applying optimum conditions are listed in the definitions of these conditions in Table 3.2. Table 3.3 (also in Section 3.2) presents nine cases to show applications of the basic and optimum conditions defined in Table 3.2, as well as intermediate conditions between basic and optimum. In these cases, any relevant RF has been applied directly to the .03 BHEP which is the combined HEP for an EOM and ECOM, another major conservatism. In all of these cases, HRA event trees were drawn as graphic aids to the calculations involved. Figure 3-4 is one such example to illustrate Case VII.

In addition to applying each RF to an EOM and ECOM as a unit, the following conservatism is used. If there is more than one component to be checked in a group of components being treated as a "system" for analysis purposes, the relevant RFs are applied to the components as a group, rather than to each component individually. This means that each RF is treated independently of the number of components in a system; each RF is counted only once to be conservative and, also, to account for the possibility that not all RFs will be employed on every occasion in which they should be employed. Thus, for any system, regardless of the number of components, the term at the end of each failure path in any HRA event tree can be multiplied by .1. This is equivalent to summing up the failure terms at the ends of all failure paths, without regard to RFs, and then multiplying the answer by the failure probability of an RF or the product of all failure probabilities of the RFs in question.

3.4.3.3 Dependence Effects for Pre-Accident Screening HRA

All of the above screening rules apply to human actions without regard to the effects of dependence. As stated previously, BHEPs must be modified



$S_T + F_T = .99997 + .00003 = 1.0$

Optimum Conditions are defined in Table 2

Figure 3-4 HRA Event Tree for Case VII in Table 3-4

for the effects of dependence. The .1 BHEP for failure of a recovery factor already includes the effects of between-person dependence between the person originally performing the task and the second person or other recovery factor. Therefore, what remains is to define screening rules for the effects of within-person dependence, that is, dependence between the tasks performed by one person (in this case, the original task performer or the recovery factor performer). For screening purposes the use of the general guidelines in Chapter 10 of NUREG/CR-1278[1] would require considerable judgement of a qualified HRA specialist for each set of tasks to be screened. Such a procedure would be unworkable in view of the hundreds of pre-accident tasks to be screened. Therefore, it was necessary to develop screening rules which could be used by systems analysts who do not have a formal background in human factors technology or HRA. For screening purposes, dependence effects are treated differently for RFs and for original task performance. For RFs, dependence effects are not specifically considered because of our rule that in any group of tasks, each RF will be applied only once. For original task performance, dependence effects are treated differently for parallel systems and for series systems. A parallel system is one in which F occurs only if all components in a system are unavailable; system success occurs as long as at least one of the components is available. A series system in one in which system success occurs only if all components in a system are available; the failure of only one component renders the entire system unavailable, and is designated as F_T. Because of the usual component redundancy in NPPs, most applications of HRA are for parallel systems when more than one component defines the system.

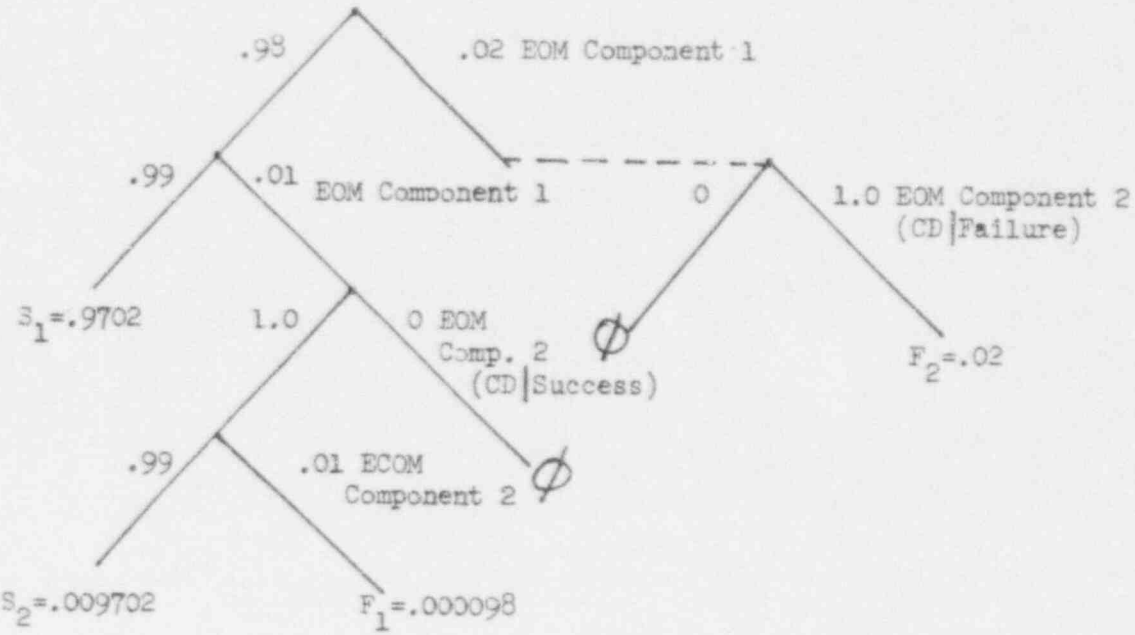
For parallel systems, zero dependence (ZD) is assumed for ECOMs while either ZD or some non-zero level of positive dependence can be assessed for EOMs. For screening conservatism, negative dependence is not used in parallel systems. For such systems, the use of positive dependence only results in conservatism. For series systems, the use of positive dependence only would result in a very small underestimation of HEPs, as long as the BHEP is not much larger than .01. The use of negative dependence would result in the most conservatism in a series system, but would add a considerable amount of complexity in the judgements required in the assessment of dependence. Furthermore, for the usual BHEPs assessed in an HRA, the use of negative dependence would add only a very small amount of conservatism as compared to an assessment of zero dependence. Consequently, for screening analysis of series systems, ZD is assessed for both ECOMs and EOMs. This seems to be a good balance between complexity avoidance and maximum conservatism. (Chapter 10 in NUREG/CR-1278[1] discusses positive and negative dependence in series and parallel systems and how to estimate their effects.)

The following discussion about assessing dependence for series and parallel systems provides a rationale for the guidelines found in Table 3.4 in Section 3.2. For series systems, ZD is always assessed. Therefore, the systems analyst can use the rules and F_ts in Table 3.3 with appropriate modification for the number of components in the system, as discussed later.

For parallel systems, it is necessary for the systems analyst to first identify those maintenance and calibration tasks for which ZD can be assessed for the EOM portions of the tasks. For those tasks for which ZD is assessed, the above rules and F_Ts in Table 3.3 are relevant, with appropriate modification for the number of components in the system, as discussed later. ZD may be assessed if there is good physical separation of the components in question (i.e., the components are not in the same visual frame of reference) and the operator is supposed to write down something (anything) for each component in question. Any two components in a related group are considered to be in the same visual frame of reference if the operator can see one of them without moving his or her head as some action is performed on the other. This assessment of ZD may be made even if the actions required for each component occur close in time, i.e., the between-action interval for each pair of related actions is less than 2 minutes. For conservatism, all related actions occurring with a between-action interval of 2 minutes or more are assessed as occurring under the zero level of dependence. The two-minute rule was adopted as a conservative modification of the one-minute guideline discussed under the heading "Functional Relationships Among Tasks" beginning on page 10-19 of NUREG/CR-1278.[1] For parallel system applications, the assessment of ZD is less conservative than a non-zero level of positive dependence, i.e., F_Ts will usually be smaller if ZD is assessed. For this reason, and especially for screening purposes, there should be a sound rationale for the assessment of the zero level of dependence when assessing parallel systems.

Next, for parallel systems, the systems analyst must identify those tasks for which non-zero levels of positive dependence are to be assessed. For screening purposes, only two non-zero levels of positive dependence are used of the four levels identified in Chapter 10 of NUREG/CR-1278.[1] The levels used are complete dependence (CD) and high dependence (HD). Assessments of low dependence (LD) and moderate dependence (MD) are not made for screening. CD is assessed if the components in question are within the same visual frame of reference, whether or not the operator is supposed to write down something for each component, and the between-action interval for each set of related actions is less than 2 minutes. HD is assessed if the between-action interval for each set of related actions is less than 2 minutes, the components in question are in the same general area, but not within the same visual frame of reference, and there is no requirement for the operator to write down something for each component. For simplicity, it is assumed that the level of dependence in any set of related actions remains constant. For example, in a three-component parallel system, if CD is assessed between the first and second components, CD should also be assessed between the second and third components. Table 3.4 in Section 3.2 summarizes these guidelines for assessing dependence.

Figure 3-5 shows the HRA event tree and calculations for $F_T \sim .02$ for the case in which there are two related components in a parallel system, and CD is assessed for the two EOMs and ZD is assessed for the two ECOMs. A parallel system is one in which F_T occurs only if both components are unavailable, in this case, from human errors. For this particular system, F_T will remain .02 for parallel systems of 3, 4, or 5 components. The



$$S_T + F_T = .979902 + .020098 = 1.0$$

Figure 3-5 HRA Event Tree for Two-Component Parallel System, CD Assessed for EOMs and ZD for ECOMs, No RFs

reason, of course, is that once the first EOM has been made, all the other components will experience an EOM probability of 1.0 because the conditional HEP, given the first EOM, is 1.0.

For Figure 3-5 and subsequent figures showing HRA event trees, the .02 and .01 BHEPs for, respectively, the original EOM and ECOM are discussed in this section. The conditional HEPs (CHEPs) assigned for non-zero levels of dependence are taken from the appropriate equations in T20-17 of NUREG/CR-1278.[1] We could have used rounded numbers, but the use of the numbers defined by the appropriate equations provides for easier traceability. It can be noted that some of the terms at the ends of success paths or failure paths in the trees are carried out to several decimal places. We do this, not because we believe such exactitude is meaningful, but because it provides a useful check on the accuracy of our arithmetic to see whether or not the sum of all end-failure and end-success terms equals 1.0 (within the limitations of the TI-55 hand calculator used for the calculations).

Figure 3-6 shows the HRA event tree for a two-component parallel system with an assessment of HD for the EOMs and the usual assessment of ZD for the ECOMs. The F_t is .01. If 3 components constitute the related set, each failure path in the tree can be extended to account for the fact that all 3 components must be unavailable. The appropriate calculations result in an F_T of .005. For 4 components, F_T = .003, and for 5 components, F_T = .001.

In Section 3.2, Table 3.5 adjusts the BHEPs from Table 3.3, modifying them for various dependence levels using the guidelines in Table 3.4, and including the effects of one through five components to be considered as a system. For series systems, ZD only is used, as discussed previously. The last column in Table 3.5 includes this modification, based on the equation

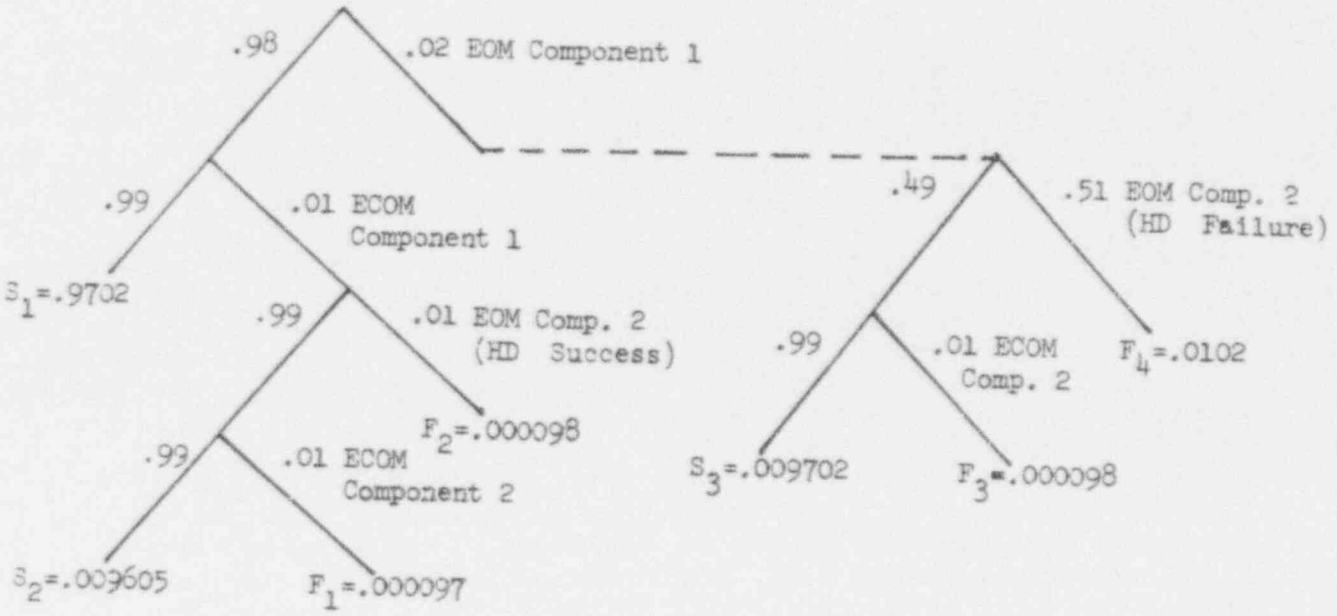
$$\text{Revised } F_T = 1 - (1 - F_T)^n$$

where n is the number of components in the series system and the F_T in parentheses is taken from Table 3.3.

For parallel systems, if ZD is assessed, see Note 2 in Table 3.5, in which the equation for total failure is

$$F_T = (F_{T,one})^n$$

where $F_{T,one}$ is the F_T for one component and n is the number of components in the system. If CD and HD are assessed, the results of the appropriate calculations are given in the table. For two-component parallel systems, the F_Ts for Case I in Table 3.5 repeat the F_Ts from the Figures 3-5 and 3-6, i.e., .02 for CD and .01 for HD. Recall that the definitions of the 9 cases are in Table 3.3 in Section 3-2, in which only Case I has no RFs.



$$S_T + F_T = .989507 + .010493 = 1.0$$

Figure 3-6 HRA Event Tree for Two-Component Parallel System, HD Assessed for EOMs and ZD for ECOMs, No RFs

The F_Ts for the other cases include the effects of the one or more RFs. As stated earlier, it is conservatively assumed that an RF applies to an EOM and ECOM as a unit. That is, in the failure path in an HRA event tree, we do not multiply the EOM by .1 and also multiply the ECOM by .1 for RFs whose HEP is .1. Instead, we multiply the F_Ts for Case I in Table 3.5 by .1 for one RF and by .1 x .1 for two RFs. The .01 failure of the PM or PC test is also a multiplier when it applies. Thus, the F_Ts for Cases II through IX in Table 3.5 are determined by straight multiplication, as shown in the left column in the table. Even with this conservatism, many of the F_Ts in the table are quite small, and should be used only after careful determination that the assumptions behind the cases in question are realistic.

Table 3.1 in Section 3.2 presents a summary of the screening procedure for the Pre-Accident HRA.

3.4.4 Final HRA Screening Rules for Pre-Accident Tasks: Set 2

When Set 1 of the final HRA screening rules for pre-accident tasks was reviewed by the RMIEP Quality Assurance (QA) Team, there was concern expressed that the screening HEPs might be too low. That is, the HEPs might be so low that important pre-accident tasks may be eliminated by the screening process. Although the SNL HRA Team did not agree with this concern, it was decided to develop a somewhat more conservative set of screening rules, based on the set presented in Section 3.4.3.3.

Set 2 of the screening rules involves the use of the upper bounds (UBs) of the estimated uncertainty bounds (UCBs) on the total-failure probabilities (F_Ts) determined from Set 1. These UBs are calculated by the application of the method for propagating UCBs in an HRA described in Appendix A of NUREG/CR-1278.[1] It is important to emphasize that this ultra-conservative screening method uses the upper bounds of the total-failure probabilities. It does not involve the use of the upper bounds for every estimated HEP that went into the calculations of the tabled numbers in Section 3.2. Such an approach would be another extreme worst-case analysis, and would amount to no screening at all.

The screening values using Set 2 were intended to be presented in parentheses in Tables 3.3 and 3.5 in Section 3.2. However, as the Set 2 screening values were not used in the RMIEP screening process, the upper bounds for Table 3.5 were not calculated, as they would have taken more time than was available on the RMIEP.

3.5 HRA Screening Rules for Post-Accident Diagnosis/Misdiagnosis

The purpose of this section is to explain or reference the rationale behind part of the HRA screening procedure for post-accident tasks presented in Section 3.3. The part described here is for the diagnosis/misdiagnosis screening HRA. The definitions of terms related to diagnosis and misdiagnosis are all defined in Section 3.3 (see especially Table 3.7). This section is divided into:

3.5.1 HRA Screening Rules for Diagnosis
3.5.2 HRA Screening Rules for Misdiagnosis

3.5.1 HRA Screening Rules for Diagnosis

For each abnormal event, the systems analysts determine T_m, the maximum allowable time to have properly diagnosed the abnormal event and to have completed the necessary human actions following T_0, the annunciation (or other compelling signal) of an abnormal event. (See Figure 3-1 in Section 3.3 for the T terms and their time relationships). T_a, the time needed to get to a particular location plus the time needed to perform the required actions once a diagnosis of an abnormal event has been made, is assessed for activities either in or outside the control room. $T_m - T_a = T_d$, the allowable time for a diagnosis. Once this time has been determined, the HEP for the T_d in question is determined from the screening diagnosis model from NUREG/CR-1278.[1] Figure 3-2 (Figure 12-3 from the Handbook) in Section 3.3 shows the model for one abnormal event. This model is the same as the one in Table 4.3-2 of NUREG/CR-2815.[11] The model represents a consensus judgement of PRA specialists, including some HRA specialists, as described in Oswald et al, 1982.[8] The background data for the consensus judgement is described on page 12-12 of NUREG/CR-1278.[1] For the case of more than one abnormal event occurring closely in time, Table 3.9 (corrected T20-1 from the Handbook) in Section 3.3 is used. The rationale for the time/HEP values for more than one abnormal event is discussed on page 12-14 of NUREG/CR-1278.[1] From that page the following definition is taken: "'Closely in time' refers to cases in which the annunciation of the second abnormal event occurs while the control room personnel are still actively engaged in diagnosing and/or planning the responses to cope with the first event. This is situation-specific, but for the initial analysis, use 'within 10 minutes' as a working definition of 'closely in time.'"

For special cases in which the need for diagnosis (including interpretation) can be considered to be nil, the lower bound curve in Figure 3-2 (or lower bound values in Table 3.9) is used. To use the lower bound values, the human behavior must be classified as skill-based rather than rule- or knowledge-based. These terms were developed by Jens Rasmussen,[10] and incorporated into the Systematic Human Action Reliability Procedure (SHARP) (EPRI NP-3583).[6] The rules for this classification are presented in Figure 3-7, taken from the SHARP document, as revised in a draft document (NUS-4531),[12] and definitions of the three terms are in Table 3.8 (in Section 3.3), taken from the SHARP document and from Rasmussen.[10] For screening purposes, the special cases are restricted to the recognition of which immediate emergency actions are required for which of the four critical parameters at the LaSalle NPP that are the entry conditions for several emergency procedures. (These four critical parameters are listed in item 9 of Table 3.6 in Section 3.3.) As judged by interviews with reactor operators and simulator instructors for the LaSalle NPP, both the entry conditions (i.e., the patterns of annunciators and other displays) and their related immediate emergency actions are committed to memory.

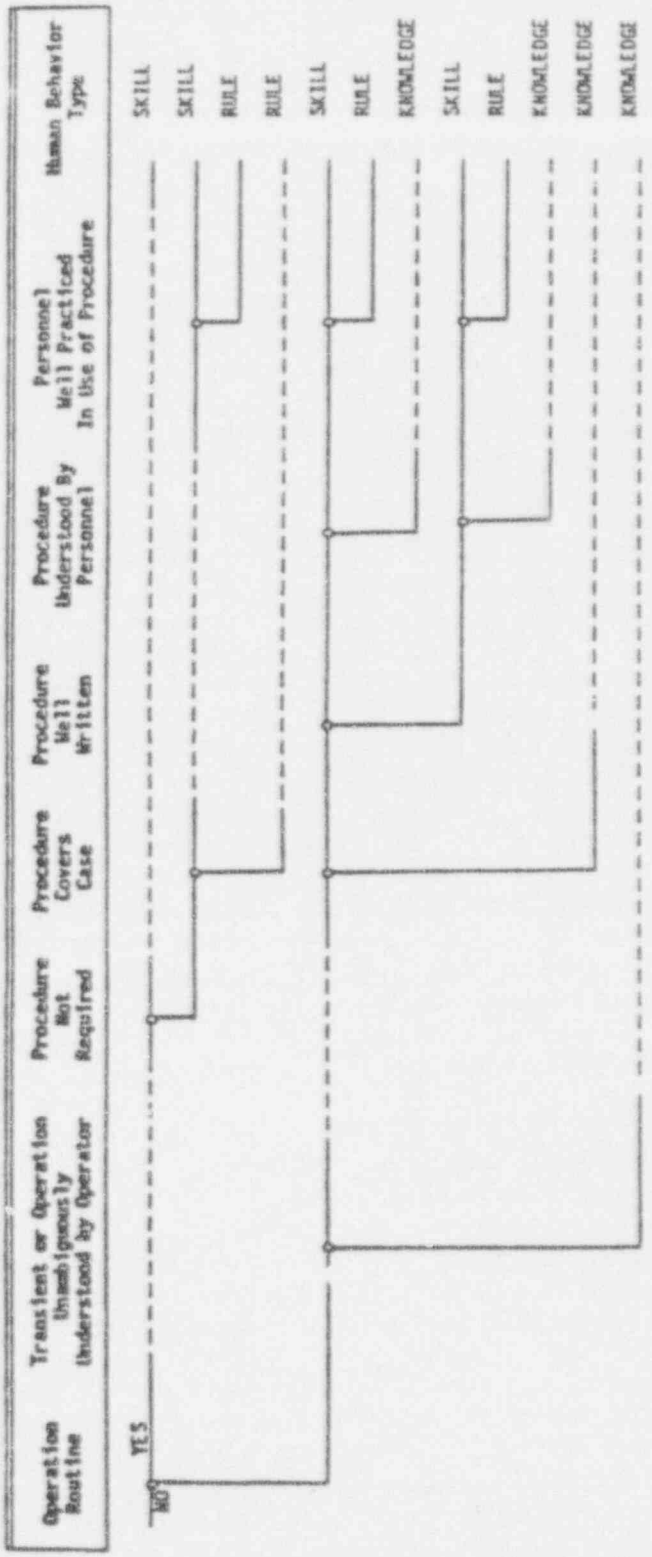


Figure 3-7 Logic Tree to Aid in Selection of Expected Behavior Type

Copy of Figure B-3 from NUS-4531

For it to be judged that the operators are using skill-based behavior, the displays of these four critical parameters must be immediately obvious, requiring absolutely no interpretation, and it must be judged that all of the skilled reactor operators (i.e., those with six or more months of experience) are so well rehearsed in this recognition of each of these critical parameters that this recognition will be essentially automatic. [Per page 18-3 of the Handbook, it is assumed that in an abnormal situation the on-duty senior reactor operator or an available skilled reactor operator would take over from any novice reactor operator (i.e., one with less than six months' experience) who happened to be manning the control room panels at the time of the abnormal event.] For screening purposes, any recognition of an abnormal event that cannot be classified as skill-based behavior is considered to be knowledge-based behavior; the category of rule-based behavior is not used for RMIEP HRA screening of post-accident diagnosis/misdiagnosis.

The HEP for diagnosis must be added to the HEP for carrying out the post-diagnosis actions (as described in Section 3.6) to obtain the total-failure probability, F_t, which is entered into the appropriate fault trees or event trees by the systems analysts. The F_t reflects the estimated screening probability that the control room personnel will fail to make the proper diagnosis and carry out the required post-diagnosis actions within T_m. These actions are those that are required to prevent core damage. The combination of HEPs and times from the diagnosis and post-diagnosis tasks is discussed in Table 3.6 in Section 3.3.

3.5.2 Misdiagnosis Screening Rules

For screening purposes, two cases of misdiagnosis are assessed, using highly conservative assumptions. For Case I, the screening diagnosis HEP assessed per Section 3.3 is considered to be equivalent to a misdiagnosis which will further result in a core damage accident. For Case II, a misdiagnosis (resulting in a core damage accident) is considered to result inevitably from cases of instrumentation failure or inaccurate instrumentation. For example, if the instrumentation tells the operator that the core is adequately covered, when it is not, we assume the operator will misdiagnose the situation, perform the wrong actions (e.g., severely limit core cooling), and thereby cause a core damage accident.

3.6 HRA Screening Rules for Post-Accident Post-Diagnosis Actions

The purpose of this section is to explain or reference the rationale behind part of the HRA screening procedure for post-accident tasks presented in Section 3.3. The part described here is for the actions which are to be carried out once a correct diagnosis has been made of an abnormal event. This section is divided into:

3.6.1 Response Time Screening Values

3.6.2 HEP Screening Values

For post-diagnosis actions, it was necessary to develop screening values for (1) the time required to carry out the actions (including travel time) and (2) the HEPs related to the actions. Also, it was necessary to consider potential credit for human actions inside and outside the control room. For conservatism, it was decided by the systems analysts not to give any credit in the HRA screening analysis for post-diagnosis actions required outside the control room. Such actions will be treated in the post-screening HRAs, i.e., the detailed or nominal HRAs. This decision was made after a visit to the plant in which travel times to locations outside the control room were determined. As a matter of interest for the nominal analysis, the next section on response times includes the results of these time measurements.

3.6.1 Response Time Screening Values

As stated above, for screening, only actions inside the control room will be used. Once a diagnosis of an abnormal event has been made, some time is required to get to the appropriate panel or panels and operate the appropriate switches or other devices. In all cases, the response time is considered to start with the completion of the diagnosis. If the control action is very simple, e.g., manipulation of one switch, a screening time of one minute is assessed. Activation of the manual trip button is a case in point. If there is a requirement to use written procedures, time is required to obtain the appropriate set. In other PRAs, it has been noted that this time may be considerable if the written procedures are not filed in a conveniently labeled and accessed place. For screening purposes, if the human actions to be performed cannot be assumed to be committed to memory and will require use of written procedures, a delay of 5 minutes is assumed before the actions will be initiated. The total amount of time for control room actions to take place depends on the number of actions and delays incurred while waiting for appropriate indications that the actions have had their intended effects. The total response times can range from one minute for a simple response to, say, 30 minutes for lengthy procedures such as boron injection. In the screening analysis, each set of human actions must be considered separately, and no attempt has been made to set down screening response times in advance of each screening HRA.

In the nominal HRAs, response times for actions to be taken outside the control room must be estimated. In anticipation of this requirement, actual travel times were measured at the LaSalle NPP by a systems analyst and an HRA specialist. For example, rapid walking time from the control room to the diesel room was 1.5 minutes, including descending some flights of metal stairs. On another measurement, from the control room to the high pressure core spray system, it was discovered that the usual path was blocked by some construction being performed on Unit 2, not in operation at that time. Even with some backtracking and a longer path, the total time was only 4 minutes. It was decided to use 6 minutes as a conservative estimate of total travel time in the screening analysis, exclusive of the time required for cases in which protective clothing and/or devices must be donned. Later, however, it was decided not to give any screening analysis

credit for actions to be taken outside of the control room. For the nominal analyses, actual measurements of rapid walking time plus simulated operation of the appropriate controls were taken in preference to reliance on estimates by operating personnel. These measures included the time required to don protective clothing and/or devices when required.

3.6.2 HEP Screening Values

Table 3.10 in Section 3.3 lists the screening HEPs for the critical actions which must be performed subsequent to diagnosis of an abnormal event. These HEPs must be added to the diagnosis HEPs, as described in Table 3.6 Section 3.3. The first item in this table lists an HEP of 1.0 for performing a required human action outside of the control room, as discussed earlier.

The second value in the table, an estimated 1.0 HEP for performing a critical skill-based or rule-based post-diagnosis action correctly when no written procedures are available, is taken from T20-2 of the Handbook. The rationale for this 1.0 HEP is that for screening purposes, it is best not to assume that operating personnel will carry out unwritten procedures correctly, even though they might be required to have memorized the actions involved. If the detailed steps required in post-diagnosis actions have not been written down, the analyst should be skeptical about the performance of the actions. This assumption was made, for example, in the nominal PRA for the Indian Point NPP for a LOCA scenario in which city water was available, but for which no written procedures were available to tell exactly were the valves were located or how to valve in the city water (Indian Point Probabilistic Safety Study, 1982).[13]

The third and fourth HEPs in Table 3.10 refer, respectively, to performing procedure-based critical actions with and without recovery factors (RFs). An initial set of higher HEPs was taken from T20-2 in NUREG/CR-1278[1] which lists a .05 HEP for failure to perform post-diagnosis rule-based actions correctly when written procedures are available and used, and .025 when recovery factors are included. These values were selected by the authors of the Handbook merely to provide a large degree of conservatism. The assessment of .025 was judged by the SNL systems analysts to be unduly conservative, and, in effect would amount to no screening at all. Therefore, the HRA analyst considered the use of the HEPs in the second half of Table 4.3-2 in NUREG/CR-2815[11] (taken from Oswald et al, 1982)[8] which lists screening HEPs of .01 for performance of a critical procedural step without immediate recovery factors, and .001 with recovery possible at the point of error action. The .001 HEP is the .01 BHEP modified for recovery factors. Note that this is equivalent to assigning a .1 failure probability for recovery factors when they are available and there is time to employ them. The .01 and .001 values were rejected as too optimistic for screening purposes, as explained on page 12-16 in the Handbook. A compromise was reached in which the .01 BHEP was designated, but modified upwards by a factor of 5 for the effects of stress, conservatively assuming that all tasks are dynamic tasks rather than step-by-step tasks. As

defined in the glossary, a step-by-step task is a "routine, procedurally guided set of steps performed one step at a time without a requirement to divide one's attention between the task in question and other tasks. With high levels of skill and practice, a step-by-step task may be performed reliably without recourse to written procedures, e.g., repairing a faucet or the sequential performance of memorized immediate emergency actions." The glossary defines a dynamic task as "one that requires a higher degree of man-machine interaction between the people and the equipment in a system than is required by routine, procedurally guided tasks. Dynamic tasks may include decision-making, keeping track of several functions, or any combination of these. A post-accident task may be classified as a dynamic task if the written emergency operating procedure is so poorly written that it is difficult to follow with ease. The operator's tasks in coping with an abnormal event may be classified either as dynamic or step-by-step tasks." In Table 3.14, a factor of 5 is used to adjust the BHEP for the effects of moderately high stress (heavy task load) on a dynamic task. These assumptions seemed sufficiently conservative for screening purposes, and the modified HEP of .05 appears as item 3 in Table 3.10.

For the case of recovery factors, the restriction made in NUREG/CR-2815[11] that the recovery must be possible at the point of error action was adopted, and the .1 BHEP from that document for the failure of the recovery action per se was modified by a factor of 2 to provide some adjustment upwards for the presumed effects of post-accident stress. The use of a factor of 2 modification is equivalent to judging that the person who is checking the first person's performance is operating more in a step-by-step manner. Thus, the value for item 4 in Table 3.10 becomes .05 x .2 = .01.

The fifth value, .001, in Table 3.10 pertains to the post-diagnosis performance of the immediate emergency actions for the four critical parameters at the LaSalle NPP which are the entry conditions for several emergency procedures. The four critical parameters, listed earlier, are: check reactor power level, check water level in the core, check reactor pressure, and check containment temperature and pressure. It is important to remember that the 001 HEP does not include the diagnosis aspect of carrying out the immediate emergency actions. As discussed in Section 3.5, for special cases which involve skill-based behavior, the lower bounds of the initial-screening diagnosis model (Figure 3-2) are used. The .001 HEP refers only to those immediate actions which must be carried out from memory after the appropriate diagnosis has been made. For the .001 HEP to apply, the conditions for skill-based behavior, as defined in Table 3.8 in Section 3.3, must be met. If these actions are not written down in an available written procedure, no credit should be given for their correct performance, as indicated in item 2 of Table 3.10.

Because the screening HEPs for diagnosis and post-diagnosis actions must be added, reference to Table 3.10 and Figure 3-2 indicates that for cases in which the post-diagnosis action HEP of .05 is used, the diagnosis HEP, rather than the post-diagnosis HEP, is dominant through about the first 25 minutes into the abnormal event. After the first 25 minutes, the post-diagnosis HEP becomes the dominant influence. If recovery factors are

Table 3.14
Modifications of Estimated HEPs for the Effects of
Stress and Experience Levels

Item	Stress Level	Modifiers for Nominal HEPs* Skilled** (a)	Novice** (b)
(1)	Very low (Very low task load)	x2	x2
	Optimum (Optimum task load):		
(2)	Step-by-step†	x1	x1
(3)	Dynamic†	x1	x2
	Moderately high (Heavy task load):		
(4)	Step-by-step†	x2	x4
(5)	Dynamic†	x5	x10
	Extremely High (Threat stress)		
(6)	Step-by-step†	x5	x10
(7)	Dynamic† Diagnosis††	.25 (EF = 5) These are the actual HEPs to use with dynamic tasks or diagnosis--they are NOT modifiers.	.50 (EF = 5)

*The nominal HEPs are those in the data tables in Part III and in Chapter 20. Error factors (EFs) are listed in Table 20-20.

**A skilled person is one with 6 months or more experience in the tasks being assessed. A novice is one with less than 6 months or more experience. Both levels have the required licensing or certificates.

†Step-by-step tasks are routine, procedurally guided tasks, such as carrying out written calibration procedures. Dynamic tasks require a higher degree of man-machine interaction, such as decision-making, keeping track of several functions, controlling several functions, or any combination of these. These requirements are the basis of the distinction between step-by-step tasks and dynamic tasks, which are often involved in responding to an abnormal event.

††Diagnosis may be carried out under varying degrees of stress, ranging from optimum to extremely high (threat stress). For threat stress, the HEP of .25 is used to estimate performance of an individual. Ordinarily, more than one person will be involved. Tables 20-1 and 20-3 list joint HEPs based on the number of control room personnel presumed to be involved in the diagnosis of an abnormal event for various times after annunciation of the event, and their presumed dependence levels, as presented in the staffing model in Table 20-4.

allowed, and the .01 HEP for post-diagnosis actions is employed, the diagnosis HEP is dominant through the first half-hour or so into the abnormal event.

Obviously, all the post-accident screening numbers are highly speculative. The values listed in Section 3.3 are intended to provide a reasonable balance between the use of unreasonably high HEPs (which would provide no screening at all) and unreasonably low HEPs (which would provide too much screening). We could have used an upper bound alternative screening method, similar to Set 2 for the HRA screening rules for pre-accident tasks (Section 3.4.4). We have not done this because we judge that the screening rules in Section 3.3 for post-accident tasks are sufficiently but not unduly conservative.

3.7 References

1. A. D. Swain and H. E. Guttmann, "Handbook of Human Reliability With Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, Albuquerque, NM, August 1983.

2. A. D. Swain, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, SAND86-1996, Sandia National Laboratories, Albuquerque, NM, February 1987.

3. L. M. Weston, D. W. Whitehead, and N. L. Graves, "Recovery Actions in PRA for the Risk Methods integration and Evaluation Program (RMIEP) Volume 1: Development of the Data Based Method," NUREG/CR-4834/1 of 2, SAND87-0179, Sandia National Laboratories, Albuquerque, NM, June 1987.

4. D. W. Whitehead, "Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP) Volume 2: Application of the Data Based Method," NUREG/CR-4834/2 of 2, SAND87-0179, Sandia National Laboratories, Albuquerque, NM, December 1987.

5. B. J. Bell and A. D. Swain, "NUREG/CR-2254 A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants," NUREG/CR-2254, SAND81-1665, Sandia National Laboratories, Albuquerque, NM, May 1983.

6. G. W. Hannaman and A. J. Spurgin, "Systematic Human Action Reliability Procedure (SHARP)," EPRI NP-3583, Electric Power Research Institute, Palo Alto, CA, June 1984.

7. G. J. Kolb, D. M. Kunsman, B. J. Bell, N. L. Brisbin, D. D. Carlson, S. W. Robertson, R. O. Wooton, S. H. McAhren, W. L. Ferrell, W. J. Galyean, and J. A. Murphy, "Interim Reliability Evaluation Program: Analysis of the Arkansas Nuclear One - Unit 1 Nuclear Power Plant, Vols 1 and 2," NUREG/CR-2787, SAND82-0978, Sandia National Laboratories, Albuquerque, NM, June 1982.

8. A. J. Oswald, C. D. Gentillon, S. D. Matthers, and T. R. Meachum, Generic Data Base for Data and Models Chapter of the "National Reliability Evaluation Program (NREP) Guide," EGG-EA-5887 Informal Report, EG&G Idaho, Inc., Idaho Falls, ID, June 1982.

9. Webster's New Collegiate Dictionary, Springfield, MA: G. & C. Merriam Co., 1975.

10. J. Rasmussen, "Models of Mental Strategies in Process Plant Diagnosis," in J. Rasmussen and W. B. Rouse (eds), Human Detection and Diagnosis of System Failures, New York: Plenum Press, 1981.

11. R. A. Bari, A. J. Buslik, A. El-Bassioni, J. Fragola, R. E. Hall, D. Ilberg, E. Lofgren, P. K. Samanta, and W. Vesely, "National Reliability Evaluation Program (NREP) Procedures Guide," NUREG/CR-2815, September 1982,

12. G. W. Hannaman, A. J. Spurgin, and Y. D. Lukic, "Human Cognitive Reliability Model for PRA Analysis," NUS-4531 (Draft), December 1984.

13. "Indian Point Probabilistic Safety Study," Power Authority of the State of New York and Consolidated Edison Company of New York, Inc., New York, 1982.

4.0 INTERSYSTEM COMMON CAUSE ANALYSIS

4.1 Introduction

Common cause failures in nuclear power plants can be subdivided into two basic categories which are determined by the initial criticality of the plant. The first category is defined as common cause failures that occur prior to initial startup. Category one is further subdivided into functional deficiencies in the engineering design; realization faults of the engineering design; and engineering construction, installation, and commissioning faults. Category two occurrences take place after initial criticality. This category is subdivided into test and maintenance procedural errors, operating procedural errors, environmental extremes, and energetic events. General guidance on the identification, modeling, and quantification of common cause events can be found in References 1, 2, 3, 4, 5, and 6.

The purpose of this section is to describe the procedure used to identify reactor plant test, maintenance, and operating procedures that have intersystem dependencies and to report the results of applying the procedure to the LaSalle nuclear power plant. The detailed results of this analysis are reported in Reference 7. Previous reactor plant risk assessments have not specifically dealt with this mode of common cause failure.

Procedure related common cause failures can be caused by errors in preventative maintenance, repair, testing after completion of repair, and routine testing. Typical causes are imperfect repair, inadequate supervision, imperfect procedures, and imperfect calibration. Imperfect repair is defined as the repair action being incomplete, or not in accordance with designated procedure. Inadequate supervision is an error due to inadequate management of the repair or testing. It also could be an error due to inadequate maintenance checking. Imperfect procedures are test, maintenance, and operating procedure construction errors which could lead to a component fault. Imperfect calibration is calibration performed incorrectly.

A study of Licensee Event Reports[8] (LERs) was conducted. This was felt to be necessary in order to obtain information that could be used to efficiently eliminate procedures that would not have a significant likelihood of having common cause interactions as part of an initial screening process. This was neccessary in order to reduce the number of procedures that would have to be evaluated in detail. It also showed areas of procedural deficiency and error in the performance of test, maintenance, and operations actions that occurred in similarly designed reactor plants that would need to be reviewed carefully for the LaSalle analysis.

With the knowledge obtained by identification of test, maintenance, and operation errors from the LER review, LaSalle procedures[9] that did not affect overall failure rates were eliminated. The procedures not eliminated were evaluated for intersystem dependencies. Since this work

was coordinated with other analysts, intrasystem common cause failures were not investigated. These possible intrasystem common cause failures were examined by the system analysts when individual system fault trees were constructed. The system analysts reviewed all the procedures that could affect their systems and identified possible procedural errors to be evaluated as described in Chapter 3 of this report.

4.2 Evaluation of Licensee Event Reports

4.2.1 Introduction

Common cause faults can be defined as faults synchronized by an external shock to the system. The level of importance of having several components fail simultaneously is such that it is vital to correctly identify when an external fault was the actual cause of failure. An explanation of how common cause faults were identified for pumps, valves, and instrumentation and control assemblies will be delineated in the following sections.

4.2.2 Common Cause Identification Method

4.2.2.1 Pumps

Most shocks affect a random number of pumps; however, there might be shocks that cause no more than one pump to be inoperable. With data examination, it can be determined whether a single pump failed on its own, or because of a shock that could have the potential for failing more pumps. An example is a pump that tripped because its outlet valve was shut. This fault could have been the result of an error in a maintenance procedure that did not call for valve repositioning. This procedural error would have the potential to cause additional pumps to be inoperable and therefore would be a common cause candidate. Another example is air binding. Air binding can affect one pump or several pumps. Therefore, all events involving air binding must be identified as potential common cause events. Both of the above examples can be intra- or inter- system depending on the exact cause of the fault. In order for procedural errors to be classified as common cause, they must have the potential, in similar circumstances, for an individual to make a mistake affecting more than one pump in a similar way so that the pumps can be considered failed at the same time (even though the operator failures may have actually taken place at different times). Multiple failures are classified as common cause only if the failures seem to be synchronized.

Similar failures discovered a few hours apart might be classified as common cause. However, this might be an erroneous conclusion. Once a potential common cause failure is discovered, the root cause of the failures must be determined in order the correctly classify the event as a single common cause failure or two independent failures that happened to be discovered at the same time.

Nearly all common cause events are restricted to single systems. This is because pumps in a single system can be of similar model and manufacture, can be in common locations, and are more often subject to common procedures. Since the pumps within a system back each other up, multiple failures can severely cripple the systems capabilities. These events are usually some of the most important events for determining the accident sequence frequencies in probabilistic risk analysis. Clearly intersystem common cause failures, if they exist, have the potential for being even more significant because of the wider potential for degradation of plant systems.

Failure rates can be estimated for pump common cause failures as described in Reference 10.

4.2.2.2 Valves

A valve can be defined as the valve body, its internal parts, and any accessories that are needed to make it functional. Supply systems to the valve operator are not considered part of the component. Failure of the supply systems is classified as a situation in which the valve does not function as designed due to external inputs or lack of inputs. An example of a command fault is electrical breaker failure for a motor operated valve. The valve has not failed, but cannot perform its designated function. Valve failure is an event where the valve itself needs repair in order to perform as designed.

Atwood identifies seven basic failure modes of valves.[11] These modes are failure to open, failure to close, internal leakage, reverse leakage, failure to operate as required, plugged or failure to remain open, and improper valve configuration. Failure to open or close occurs when a valve fails to open or close fully when required to do so. This would include safety relief valves not reseating. Internal leakage is defined as a valve showing fully closed, but there is a measurable leak rate past it. Reverse leakage only applies to check valves. This mode describes internal leakage in this case. Failure to operate as required is reported when a valve cannot meet its opening or closing time specifications, or the valve cannot adequately control system parameters. The plugged designation is applied when flow is limited or completely stopped through a normally open valve. Improper configuration designates events caused by human factors. These types of events are considered command faults.

The same criteria applied to pumps can be used for valves. This criteria is whether an external shock caused or could have caused simultaneous failures. Once again, a shock might cause only one valve to fail. An example of a potential common cause failure is a valve that has been manually torqued down too tightly. Another example is a motor operated valve that has its breaker not racked in properly. These failures could be classified as command faults since they occur due to personnel error. For these events to be classified as common cause, it must be plausible for similar events to occur to other valves at some other time due to the same

mechanism. Design errors are usually not classified as common cause due to the absence of a synchronization mechanism.

4.2.2.3 Control and Instrumentation Assemblies

Instrumentation and control assemblies are comprised of many dissimilar components. Each component would not have more than a few observable failures, if any at all. This aforementioned fact leads to the necessity for treating this data differently from pump or valve mechanical failure. Components are, therefore, grouped into units or "super events" for representation and analysis in the PRA. Units can be grouped depending upon whether they perform digital or analog functions.

A digital unit is comprised of a sensing device and is possibly equipped with a trip device. Examples of this type of unit are pressure and level monitoring devices.

An analog unit utilizes one or more sensing detectors. Parameters monitored are typified by neutron flux, flow, or temperature instruments. The sensing device is composed of wires, amplifiers, diodes and other components. Sensing devices in LERs are coded as a sensor or a transmitter. The output of the sensing device is passed through cables to intermediate stage devices. These devices could possibly amplify, condition, or convert the signal. An example of a converter frequently encountered is those in the source range power level detection units. Input pulses are converted into a square wave output signal through the use of either a monostable or bistable multivibrator. The resulting output signal is sent to indicating devices and comparators. Comparators generate an off or on output signal depending upon a comparison with a reference signal. An analog unit can be composed of all the aforementioned components. Analysis of analog units is complicated due to channel-to-channel variance. This fact is exemplified by the amount reactor coolant flow sensors vary even with the same plant designer.

Units are considered as independent entities only if they can act independently with no common components. Most analog units are broken into two parts. These parts are the sensing device and the signal conditioning components. There is one exception to this rule. Main steam line radiation monitoring units share no components with any other channel; therefore, there is no reason to further subdivide them.

Fault rates could be estimated for the subdivisions of control and instrumentation assemblies.[12] These subdivisions are analog channel sensing devices, analog conditioning components, digital channels, and main steam line radiation monitors.

4.2.3 Failure Due to Administrative Error

One other major area of common cause failure was found. This area was failure to perform prescribed maintenance on time and maintenance schedules

which did not accurately reflect plant specifications. Even with quality assurance audits and computerized maintenance scheduling, this error was found in a significant proportion of the identified LERs. Since this error was random, a calculated failure rate could be determined for all plant components as a whole. However, it is not clear if failure to perform maintenance would lead to a component failure. It is possible, however, that a previously failed component or system would either remain undetected for a longer than normal time interval (in general this would be corrected by a shorter interval for the next maintenance) or, if the failure had been detected, result in a larger unavailability (this should be reported in the distribution of times for maintenance outages in the data base).

4.2.4 Difficulties With Using LERs as a Data Base

Using LERs as a data base presented two major difficulties. The first difficulty was in obtaining sufficient data to correctly analyze the event. For example, in one LER the number of failed assemblies is not given. An assignment of some number of failed assemblies cannot arbitrarily be inferred. Another data base imperfection is that some LERs provide incomplete information as to the case of failure. This lack of complete information could lead to some amount of incorrect designation. To minimize this effect, each of the LERs designated as common cause failure was checked twice to insure consistency and accuracy.

The second difficulty arose from the plant-to-plant variance in reporting policy. Some plants had as many as five times the amount of reports as others for the same time increment. One plant's high reporting rate does not necessarily correlate to a higher failure rate than another plant with fewer reports. Comparison of plant reporting rates should be viewed with much skepticism. How important a contribution these variations have on the data base is unknown. Reporting requirements also led to another problem. The policy is to submit reports only when a safety requirement has been violated. A potential problem is that one channel of instrumentation could be bypassed without a LER being issued. For instance, technical specifications require two out of three operable average power range monitors per channel. One average power range monitor being bypassed would not be reported unless there was another failure.

4.3 Evaluation of LaSalle Test and Maintenance Procedures

Errors repeated during maintenance and testing activities can result in unavailability of one or more systems. Limit switches could be set incorrectly on valves of more than one system or on redundant trains of one system. Valve actuators would be damaged and possibly disable valves in more than one safety system. Similar types of errors could occur during testing.

Failure rates can be estimated in two steps. In the first step the procedure is reviewed to flag actions or groups of actions which, if

performed incorrectly, would disable the component. Secondly, failure probabilities for the key actions are summed. This will give an estimate of a component's failure probability, if a test or maintenance procedure is performed. Conditional failure probabilities for these basic events are not usually independent. The dependence occurs because performance of a task on one component will affect the ability to repeat the task on another component.

The failure rate is the product of the frequency of an activity's performance and the probability, given performance of the activity, that all components will fail. Frequencies for testing can be identified from the applicable procedures and vary from shiftly to once every eighteen months. Maintenance frequencies can be determined from utility data.

Test and maintenance procedures were eliminated on the basis of being non-safety system related or that they did not involve systems within the scope of the LaSalle probabilistic risk assessment. This step reduced the amount of procedures needing detailed review by roughly a factor of ten. Three hundred and sixty seven procedures remained within the scope of the analysis.

Procedures identified for detailed analysis are listed in Appendix B. It was found that most of the intersystem dependencies occurred in electrical test and maintenance procedures. This is exemplified by LOP-AP-14 which tests all plant 6.9 and 4.16 kV transformers. Mechanical system procedures contributed less than 10 percent to possible intersystem failures.

4.4 Analysis of Plant Operating Procedures

Errors of omission and commission by plant operators can lead to common cause failure. Most errors occur in emergency situations, but some can occur while performing non-emergency operating procedures.

Atwood identified the failure rate as the product of two quantities.[1] These quantities are the frequency for task performance and probability of failure provided that a task is performed. Frequencies for task performance are either given in the operating procedures or can be obtained in consultation with plant personnel.

The operating procedure is evaluated to identify actions where operator error could occur. Potential errors should be identified for each action. Most procedures require only satisfactory completion of a few actions. After the potential errors are identified, an event tree can be constructed as described in Chapter 3 of this report. Errors are modelled in the sequence in which they occur. Every path through the tree signifies a potential outcome. By review of the operating requirements, success or failure for each outcome can be identified.

Operating procedures are identified in Appendix B on the basis of whether or not intersystem dependencies occur. Most intersystem dependencies

occurred in electrical procedures. Typical electrical procedures were racking in a circuit breaker, changing an electrical system lineup, electrical lineup verification checklists, and ground isolation.

Racking in circuit breakers has the potential, if performed incorrectly, of affecting many systems on a plant wide basis. Two steps of the procedure are identified as being critical to its correct performance. One step is replacement of the trip and close fuse blocks. The other step is the operation of the racking wrench until the breaker stop is reached.

Changing electrical system lineups was identified as having intersystem dependencies in five procedures. Four of these procedures affected the AC distribution system, while the other affected the DC distribution system. Typical critical steps in AC distribution system procedures include opening and closing of circuit breakers, changing the operating mode of diesel generators, and alteration of power supply feeds to distribution panels. In the DC distribution system procedure, two key steps are flagged. These steps are transfer of power between the alternate and normal sources and verification of battery charger output voltage.

Electrical system lineup verification checklists mostly check single systems. These checklists were eliminated from consideration. Two 125 VDC checklists were not eliminated because of identified intersystem dependencies. Some of these dependencies are verification checks of control power to thirteen switch gears, control power for feed pump control, and power to the ADS, RCIC, RHR, and LPCS interlock panels.

Ground location and isolation checks are identified due to the very nature of the procedure. Grounds are checked by de-energizing a load of whatever power bus is being investigated. If after concluding that the aforementioned load is not the source of the ground, it should be re-energized. There is a possibility that loads could remain secured by incorrect performance of the previous step.

Seven mechanical procedures which had intersystem dependencies are identified. Most of these intersystem dependencies occurred between the RHR, LPCS, and RCIC systems. Since mechanical procedures contain significant variance, generalizations about key steps cannot be derived. These procedures must, therefore, by analyzed on an individual basis. A brief summary of intersystem dependencies for mechanical procedures is included in Appendix B on a procedure-by-procedure basis.

Logic and relay checking instrument maintenance surveillances, with the exception of the high drywell pressure logic check, were found to have no intersystem dependencies. In the drywell pressure check, logic setpoints are calibrated for the LPCS, RHR (LPCI Mode), ADS, and RCIC systems. Since the same calibration steps exist for each system, a possible common cause failure can occur.

Among the operating surveillances, the shiftly surveillance is considered to be the procedure with the greatest likelihood of common cause failure

occurrence. This procedure checks indications from the core protective trip instruments control rod drive system, motor driven reactor feed pump, diesel generators, HPCS system, RHR system, LPCS system, service water system, and standby gas treatment system. Incorrect performance of some steps could lead to common cause failure.

4.5 Conclusions

Not many intersystem dependencies exist in test and maintenance procedures. The majority of dependencies are in electrical procedures. It is felt that revision of these electrical procedures is not warranted. For example, procedures for checking for grounds cannot be altered. A checklist of all affected loads is performed at the conclusion of this procedure. There will always be some small probability that a load is not returned to service. This probability could be altered significantly by factors other than the way the procedure is written. One important factor could be having a different operator perform the checklist from the one who performed the ground isolation steps. Another way to minimize failure would be to have a second operator independently perform the checklist.

One area of improvement might be warranted. This is the area of administrative control of test and maintenance procedures. More careful review and auditing could eliminate a significant amount of procedures not being accomplished in the allotted time frame and procedures not conforming to the technical specifications.

The identified common cause failures were inserted as events in the fault trees at the appropriate place so that their effects would propagate up through the fault trees and affect the front-line systems used to mitigate the accidents appropriately.

4.6 References

1. C. L. Atwood, "Estimators for the Binomial Failure Rate Common Cause Model," NUREG/CR-1401, EGG-EA-5112, Idaho, Inc., Idaho Falls, ID, April 1980.

2. C. L. Atwood, "Data Analysis Using the Binomial Failure Rate Common Cause Model," NUREG/CR-3437, EGG-2271, EG&G Idaho, Inc., Idaho Falls, ID, 1983.

3. C. L. Atwood and W. J. Suitt, "User's Guide to BFR, A Computer Code Based on the Binomial Failure Rate Common Cause Model," NUREG/CR-2729, EGG-EA-5502, EG&G Idaho, Inc., Idaho Falls, ID, February 1983.

4. A. M. Kolaczkowski, A. C. Payne, Jr., "Station Blackout Accident Analysis (Part of NRC Task Action Plan A-44)," NUREG/CR-3226, SAND82-2450, Sandia National Laboratories, Albuquerque, NM, May 1983.

5. D D. Carlson, et al., "Interim Reliability Evaluation Program Procedures Guide," NURER/CR-2728, SAND82-1100, Sandia National Laboratories, Albuquerque, NM, January 1983.

6. "Dependent Failure Analysis Procedures Guide," JBF Associates, Inc., Knoxville, TN, 1984.

7. J. A. Lambright, "Common Mode Failure Analysis of Test and Maintenance Procedures at LaSalle Unit #2 Boiling Water Reactor Plant 5/Mark II," B.S. Thesis, University of Illinois, Urbana, Ill., 1984.

8. "Licensee Event Reports," Division of Licensing, Office of Nuclear Reactor Regulation, US Nuclear Regulatory Commission, Washington, DC, 1983.

9. LaSalle Test and Maintenance Procedures, Commonwealth Edison Company, Chicago, Il, 1981.

10. C. L. Atwood, "Common Cause Fault Rates for Pumps," NUREG/CR-2098, EGG-EA-5289, EG&G Idaho, Inc., Idaho Falls, ID, February 1983.

11. J. A. Steverson, C. L. Atwood, "Common Cause Fault Rates for Valves," NUREG/CR-2770, EGG-EA-5486, EG&G Idaho, Inc., Idaho Falls, ID, February 1983.

12. T. R. Meachum and C. L. Atwood, "Common Cause Fault Rates for Instrumentation and Control Assemblies," NUREG/CR-3289, EGG-2258, EG&G Idaho, Inc., Idaho Falls, ID, May 1983.

APPENDIX A

BACKGROUND OF BASIC HEPs FOR PRE-ACCIDENT HRA

A.0 Introduction

The purpose of this appendix is to show the sample human reliability analyses (HRAs) behind the screening human error probability (HEP) of .02 for errors of omission (EOMs) and .01 for errors of commission (ECOMs). These screening HEPs of .02 and .01 are considered basic HEPs and are used in Section 3.4.3 in the main body of this report.

The next three sections present sample HRAs to illustrate the rationale behind the basic HEPs. The individual HEPs in the HRA event trees in these sections are based on the "Revised Preliminary Screening Rules," Section 3.4.2. All references to tabled data are to tables in Chapter 20 of the revised NUREG/CR-1278, dated Aug. 1983. As in Chapter 3 of this report, a table reference such as T20-22 #1, refers to data item #1 in Table 20-22. Human success probabilities (HSPs) are shown on left-hand limbs and HEPs are shown on right-hand limbs of the HRA event trees, as described in Chapter 5 of NUREG/CR-1278. Error factors (EFs) are shown with their related HEPs. Consistent with reliability analysis techniques used in the Reliability Department, Sandia National Laboratories, since 1951, final rounding of the total-failure term, F_T, is done, but the intermediate failure terms are not rounded, giving them the appearance of "pseudo-accuracy." Thus, in the HRA event trees in this appendix, the end-failure terms (i.e., the terms at the ends of failure paths through the tree) are not rounded. This approach enables the analyst to make a useful check to see that the sum of all success and failure paths through a tree sum to 1.0, within the limitations of the calculator being used.

The two-page Figure A-1 is a copy of a Piping and Instrumentation Diagram (P&ID) for the Standby Liquid Control (SBLC) System which the systems analysts and HRA specialist used to identify and analyze man-machine interfaces. The sections which follow refer to equipment items in this P&ID.

The paragraph numbering system used in performing the HRAs is used in each section. This system is convenient for cross referencing.

A.1 Total-Failure HEP #1 for Screening Pre-Accident HRA

1. Subject: Screening Analysis of Standby Liquid Control (SBLC) System Pump Flow Monthly Test.

2. Critical Steps From Following Procedure:
   LOS-SC-M1, Rev. 8: SBLC Pump Flow Test Inservice Test and Explosive Valve Continuity Check.

   [Note: The quoted procedures in this appendix are printed as they appear in the LaSalle plant procedures, except for differences in spacing and line lengths. The relevant sheet from the recording form, Attachment 2A, appears as Figure A-2. When there is second person verification, this is indicated by the box labeled "2nd."]

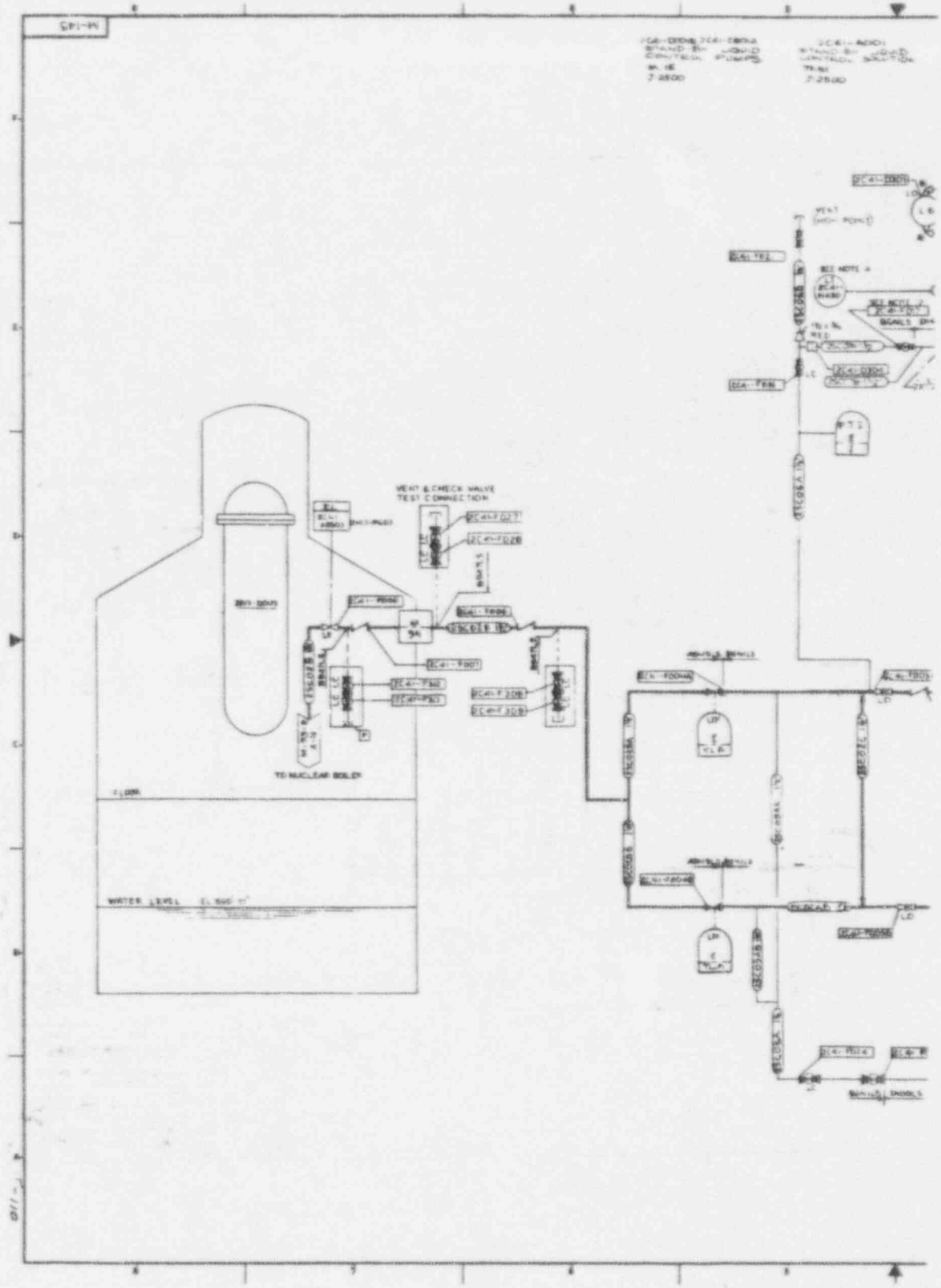


Figure A-1 SBLC P&ID for the HRAs

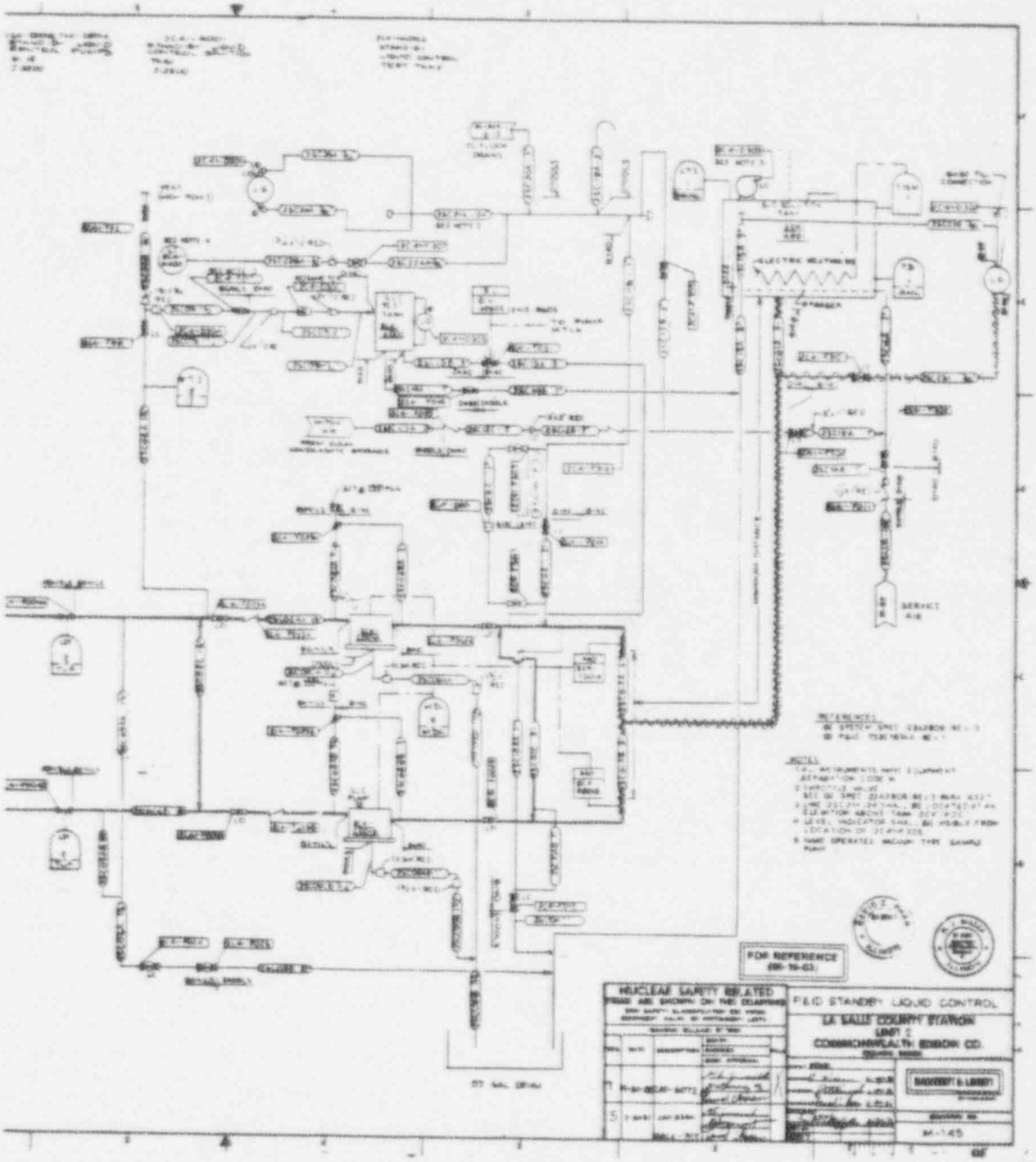


Figure A-1 SBLC P&ID for the HRAs (Concluded)

ATTACHMENT 2A

SIGNOFF SHEET

SBLC PUMP FLOW TEST, INSERVICE TEST AND EXPLOSIVE VALVE CONTINUITY CHECK - UNIT 2

PARAGRAPH NUMBER	DESCRIPTION	LIMITS	OBSERVED VALUE	OPERATOR INITIALS
F.4.i	SBLC Pump A Relief Valve 2C41-F029A	Required Value Fully Closed (T.S. 4.1.5.c.3		
	SBLC Pump B Relief Valve 2C41-F029B	Required Value Fully Closed (T.S. 4.1.5.c.3)		
F.4.j	SBLC Pump Instrument I.D. 2C41-C001A Number and Type Vibration	Acceptable: 0.40 in/sec Alert Range: .40 in/sec to .80 in/sec Required Action: .80 in/sec INSTRUMENT ID#	HIGHEST VALUE _____ in/sec ID# _____	
	SBLC Pump 2C41-C001B Vibration	Acceptable: 0.44 in/sec Alert Range: .44 in/sec to .66 in/sec Required Action: .66 in/sec INSTRUMENT ID#	_____ in/sec ID# _____	
F.4.k	Explosive valve flange leakage	NO LEAKAGE		

Figure A-2 Attachment 2A to LOS-SC-M1, Rev. 8

ATTACHMENT 2A
SIGNOFF SHEET
SBLC PUMP FLOW TEST, INSERVICE TEST AND EXPLOSIVE
VALVE CONTINUITY CHECK - UNIT 2

PARAGRAPH NUMBER	DESCRIPTION	LIMITS	OBSERVED VALUE		OPERATOR INITIALS	
			1st	2nd	1st	2nd
F.5.a	2C41-F016 Position after relocking	LOCKED CLOSED				
F.5.b	2C41-F017 position	CLOSED				
F.5.c	2C41-F031 Position after relocking	LOCKED CLOSED OPEN Indication OFF				
F.6	2C41-F301 Position after relocking	LOCKED OPEN	1st	2nd	1st	2nd
F.9.a	2C41-F008, SBLC Injection Line Stop	OPEN light indication (T.S. 4.1.5.b.4)				
F.9.b	2C41-F001A and 2C41-F001B SBLC Pump Suction Stops	CLOSED light indication (T.S. 4.1.5.b.4)				
F.10	SBLC Test Tank Sample Taken by Rad Chem (Flush per LOP-SC-07 if unsat)	Sample Taken				
F.11	SBLC System lined up in accordance with LOP-SC-02, second verif. of valves on this Att. complete	Complete				

Figure A-2 Attachment 2A to LOS-SC-M1, Rev. 8 (Concluded)

2.1 "5. Align the valves as follows at the SBLC station and RECORD valve positions on the Attachment 1A(2A).

[Note: As the HRA pertains to Unit 2 at the plant, Attachment 2A rather than 1A is used, and the prefix "2" rather than "1" is used for equipment numbering.]

[Note: The practice of using one set of procedures for two units results in a material decrease in ease of reading, with a resultant increase in reading errors. In INPO documents this practice is not recommended. Thus, in the step which follows, 1C41-F016 would be written, but not its corresponding unit 2 term, 2C41-F016.]

a. CLOSE SBLC Test Tank Inlet Upstream Stop, 1C41-F016 (2C41-F016) and LOCK.

b. CLOSE SBLC Test Tank Inlet Downstream Stop, 1C41-F017 (2C41-F017).

c. CLOSE SBLC Test Tank Outlet Stop, 1C41-F031 (2C41-F031) and LOCK."

2.2 "8. At panel 1H13-P603 (2H13-P603), OBSERVE that 1C41- F031 (2C41-F031), OPEN light is not lit."

[Note: This panel is in the control room, and serves as recovery for error in step 5.c above.]

2.3 "11. VERIFY the SBLC Control System lined up for Standby Operation in accordance with LOP-SC-02. Have second operator VERIFY valve positions as indicated on Attachment 1A(2A) and RECORD on Attachment 1A(2A)."

[Note: With few exceptions, no recovery credit was given in this HRA for operator self-verification, but credit was given for second operator verification for errors in step 5.a, the only one of the three steps in which second operator verification is required.]

2.4 "12. DOCUMENT the time of completion on Attachment 1A(2A). VERIFY all data blanks are properly filled in or noted as N.A. (not applicable) and forward to the Shift Supervisor for review and routing per Attachment 1A(2A)."

[Note: No recovery credit is given for either the self-verification by the operator for checking preformed by the shift supervisor for unfilled-in blanks.]

3. Assumptions and Notes:

3.1 For Operator A, nominal HEPs were used. When in doubt, the worst nominal HEP from an HEP table was used.

3.2 For Operator B (i.e., for verification by a second person of the status of equipment), an HEP = .1 was used (from T20-22 #1).

3.3 For self-verification, generally no error recovery credit was given. If a later step in a procedure calls for checking a separate item of equipment to verify errors made on some other items of equipment (e.g., checking a status lamp in the control room to verify valve position), an HEP = .1 was used for screening purposes only.

3.4 Failure to perform the test was not included in the HRA because it is presumed not to impact unavailability directly.

3.5 Half of the operators will misuse the provisions in Attachment 2A which calls for writing down valve positions, i.e., half of them will not refer to Attachment 2A immediately after the completion of a relevant step in the written procedure, the LOS.

3.6 One operator will do the entire procedure on his or her own, and a second operator will then verify valve positions as specified in Attachment 2A by reference to the "2nd boxes."

3.7 No extra credit was given for the fact that valve position verification is hands-on rather than merely visual.

3.8 No recovery credit was assigned to the shift supervisor for checking Attachment 1A for unfilled-in blanks.

4. Pre-Accident Generic HRA Event Tree #1 (Figure A-3):

Operator restores a locally-operated valve after a periodic test, correct written procedures to be used consisting of a long list (i.e., > 10 items), valve position to be written down on a separate recording form, and selection errors are possible.

5. HEP Screening Estimates:

5.1 Manual valve 2C41-F031 (SBLC Test Tank Outlet Stop) left open. Op A HEP = .02. OP A display verification = .1. Joint HEP (JHEP) = .002.

5.2 Manual valves 2C41-F016 (SBLC Test Tank Inlet Upstream Stop) and F017 (SBLC Test Tank Inlet Downstream Stop throttle valve) both left open.

(Note: Zero Dependence is assumed for errors of omission between the two written steps for these valves because of the influence of Attachment 2A, and the physical separation of the valves.)

$S_T + F_T = .9814118 + .0185883 = 1.0000001.\ F_T = .02.$

Figure A-3 Pre-Accident Generic HRA Event Tree #1

Op A HEP = (.02) for both valves. Op B verification for F016 = .1 HEP. Therefore,

JHEP = .0004 x .1 = 4 x 10,

the probability that both valves will be left open and not recovered.

A.2 Total-Failure HEPs #2, #3, and #4 for Screening Pre-Accident HRA

1. Subject: Screening Analysis of Three-Year Explosive Valve and Injection Test.

2. Human Errors:

2.1 Error #1 - Leave in disconnected state, valve 2C41-F004A and/or F004B.

2.2 Error #2 - Fail to close breakers for inlet motor operated valves (MOVs) 2C41-F001A and/or F001B.

2.3 Error #3 - Fail to open outlet maintenance manual valve 2C41-F008.

3. Critical Steps from Following Procedures:

LOS-SC-R1, Rev. 6: Standby Liquid Control System Injection Test

LOS-SC-M1, Rev. 8: SBLC Pump Flow Test Inservice Test and Explosive Valve Continuity Check Attachments 1A(2A) for each written procedure included as Figures A-4 and A-5.

3.1 Critical Steps in Procedure for Human Error #1:

"F.17. After the Explosive Valve has been replaced and the outage is cleared, RETURN the SBLC System to service as follows:

b. VERIFY both Explosive Valve cables are connected to the Explosive Valves. RECORD on Attachment 1A(2A)."

"F.19. PERFORM the SBLC Pump Flow Test, Inservice Test, and Explosive Valve Continuity Check per LOS-SC-M1."

[Note: The following step from LOS-SC-M1 is a recovery factor for an error in step F.17.b above in LOS-SC-R1.]

"F.1. At Control Room Panel 1H13-P603 (2H13-P603), CHECK continuity of explosive charges for SBLC Squib valves, 1C41-F004A and 1C41-F004B (2C41-F004A and 2C41-F004B), as follows:

ATTACHMENT 2A

UNIT 2 SBLC INJECTION TEST SIGNOFF SHEET

PARAGRAPH NUMBER	DESCRIPTION/LIMITS	REQUIRED VALUE	OBSERVED VALUE	OPERATOR INITIALS
F.1	EPN of Explosive Valve to be tested	N/A	EPN of Valve to be tested is _____	
F.1	EPN of SBLC Pump to be run for injection test	N/A	EPN of Pump to be run is _____	
F.5.a	SBLC Pump Motor Operated Suction Stop, 2C41-F001A, Breaker.	OPEN		
F.6.a	SBLC Pump Motor Operated Suction Stop, 2C41-F001B, Breaker	OPEN		
F.7.a	SBLC Solution Tank Level	N/A		
F.7.c	2C41-F031, SBLC Test Tank Outlet Stop, position prior to unlocking.	LOCKED CLOSED		
F.7.e.2.a	2C41-F014, SBLC Head Tank Stop, position prior to unlocking.	LOCKED CLOSED		
F.7.e.2.f	2C41-F014, SBLC Head Tank Stop, position after relocking.	LOCKED CLOSED		

Figure A-4 Attachment 2A to LOS-SC-R1, Rev. 6

ATTACHMENT 2A

UNIT 2 SBLC INJECTION TEST SIGNOFF SHEET

PARAGRAPH NUMBER	DESCRIPTION/LIMITS	REQUIRED VALUE	OBSERVED VALUE	OPERATOR INITIALS
F.14	2C41-F031 position indicated at 2H13-P603	Indicated FULLY CLOSED		
F.15.a.1	2C41-F008, SBLC Injection Line Stop, position prior to unlocking.	LOCKED OPEN		
F.15.e.1	2C41-F003A, SBLC Pump Discharge Stop, position prior to unlocking.	LOCKED OPEN		
F.15.f.1	2C41-F003B, SBLC Pump Discharge Stop, position prior to unlocking.	LOCKED OPEN		
F.17.a.3.b	2C41-F008, SBLC Injection Line Stop, position after relocking.	LOCKED OPEN		
F.17.a.7.b	2C41-F003A, SBLC Pump Discharge Stop, position after relocking.	LOCKED OPEN		
F.17.a.8.b	2C41-F003B, SBLC Pump Discharge Stop, position after relocking.	LOCKED OPEN		
F.17.b	Explosive Valve, 2C41-F004A and 2C41-F004B Cables	CONNECTED TO VALVE		
F.17.c	SBLC System Lineup	SBLC SYSTEM LINED UP PER LOP-SC-02		

Figure A-4 Attachment 2A to LOS-SC-R1, Rev. 6 (Concluded)

ATTACHMENT 2A

SIGNOFF SHEET

SBLC PUMP FLOW TEST, INSERVICE TEST AND EXPLOSIVE VALVE CONTINUITY CHECK - UNIT 2

PARAGRAPH NUMBER	DESCRIPTION	LIMITS	OBSERVED VALUE	OPERATOR INITIALS
F.1.a	SBLC Explosive Valve Continuity Check 2C41-F004A	Required Condition READY Light Is Lit (T.S. 4.1.5.b.2)		
F.1.a	SBLC Explosive Valve 2C41-F004B Continuity Check	Required Condition READY Light is Lit (T.S. 4.1.5.b.2)		
F.2.a	SBLC Pumps Manual Suction Stop 2C41-F002A-B and Discharge Stops 2C41-F003A-B	LOCKED OPEN		
F.2.b	SBLC Pumps MO Suction Stop 2C41-F001A-B	CLOSED		
F.2.c	2C41-F016 Position prior to unlocking	LOCKED CLOSED		
F.2.f	2C41-F031 Position prior to unlocking	LOCKED CLOSED		
F.3.b.1	2C41-F014 Position prior to unlocking	LOCKED CLOSED		

Figure A-5 Attachment 2A to LOS-SC-M1, Rev. 8

ATTACHMENT 2A

SIGNOFF SHEET

SBLC PUMP FLOW TEST, INSERVICE TEST AND EXPLOSIVE VALVE CONTINUITY CHECK - UNIT 2

PARAGRAPH NUMBER	DESCRIPTION	LIMITS	OBSERVED VALUE	OPERATOR INITIALS
F.4.i	SBLC Pump A Relief Valve 2C41-F029A	Required Value Fully Closed (T.S. 4.1.5.c.3		
	SBLC Pump B Relief Valve 2C41-F029B	Required Value Fully Closed (T.S. 4.1.5.c.3)		
F.4.j	SBLC Pump Instrument I.D. 2C41-C001A Number and Type Vibration	Acceptable: 0.40 in/sec; Alert Range: .40 in/sec to .80 in/sec; Required Action: .80 in/sec; INSTRUMENT ID#	HIGHEST VALUE _____ in/sec ID# _____	
	SBLC Pump 2C41-C001B Vibration	Acceptable: 0.44 in/sec; Alert Range: .44 in/sec to .66 in/sec; Required Action: .66 in/sec; INSTRUMENT ID#	_____ in/sec ID# _____	
F.4.k	Explosive valve flange leakage	NO LEAKAGE		

Figure A-5 Attachment 2A to LOS-SC-M1, Rev. 8 (Continued)

ATTACHMENT 2A
SIGNOFF SHEET
SBLC PUMP FLOW TEST, INSERVICE TEST AND EXPLOSIVE VALVE CONTINUITY CHECK - UNIT 2

PARAGRAPH NUMBER	DESCRIPTION	LIMITS	OBSERVED VALUE		OPERATOR INITIALS	
			1st	2nd	1st	2nd
F.5.a	2C41-F016 Position after relocking	LOCKED CLOSED				
F.5.b	2C41-F017 position	CLOSED				
F.5.c	2C41-F031 Position after relocking	LOCKED CLOSED OPEN Indication OFF				
F.6	2C41-F301 Position after relocking	LOCKED OPEN	1st	2nd	1st	2nd
F.9.a	2C41-F008, SBLC Injection Line Stop	OPEN light indication (T.S. 4.1.5.b.4)				
F.9.b	2C41-F001A and 2C41-F001B SBLC Pump Suction Stops	CLOSED light indication (T.S. 4.1.5.b.4)				
F.10	SBLC Test Tank Sample Taken by Rad Chem (Flush per LOP-SC-07 if unsat)	Sample Taken				
F.11	SBLC System lined up in accordance with LOP-SC-02, second verif. of valves on this Att. complete	Complete				

Figure A-5 Attachment 2A to LOS-SC-M1, Rev. 8 (Concluded)

a. CHECK that SQUIB VALVE READY lights are lit and NOTE on SBLC Pump Flow Test, Inservice Test and Explosive Valve Continuity Check Sign-Off Sheet, Attachment 1A(2A)."

[Note: It is assumed that neither step F.4.k (observe squib valve flanges for leakage) nor step F.19.d (verify external leakage at explosive valves) is a recovery factor for step F.17.b above.]

3.2 Critical Steps in Procedure for Human Error #2:

"F.17. After the Explosive Valve has been replaced and the outage is cleared, RETURN the SBLC System to service as follows:

a. CLEAR the out-of-service on the following SBLC System components and position as follows.

1) SBLC Pump Motor Operated Suction Stop, 1C41-F001A (2C41-F001A), Breaker - CLOSED.

2) SBLC Pump Operated Suction Stop, 1C41- F001B (2C41-F01B), Breaker - CLOSED."

[Note: The closing of these breakers is not entered on Attachment 1A(2A), yet the opening of the breakers in steps F.5.a and 6.a was recorded on the attachment.]

[Note: Perhaps the following step provides some recovery factor for an error in F.17.a, but we do not have LOP-SC-02 to evaluate this possibility.]

"F.17.c. VERIFY that the SBLC System is lined up per LOP-SC-02, Standby Operation of the SBLC System. RECORD that the SBLC System lineup was checked per LOP-SC-02 on Attachment 1A(2A)."

[Note: Step 19 in LOS-SC-R1 states to perform the monthly pump test per LOS-SC-M1. Step F.2.b in the latter procedure states to verify that the two MOVs (F001A and B) are closed. Since these MOVs are normally closed, this check, if made directly at the MOVs, will not catch an error in F.17.a above. The check would catch this error if, instead of looking directly at the MOVs, the operator calls up to the control room and asks if the CLOSED lamps are lit. We will assume that the operator does not follow the latter procedure, and so we assign no recovery factor here.]

[Note: A later step in LOS-SC-M1 does provide a good recovery factor, as follows.]

"F.9. At panel 1H13-P603 (2H13-P603), CHECK the following and RECORD on Attachment 1A(2A).

b. Closed light indication for 1C41-F001A (2C41-F001A) and 1C41-F001B (2C41-F001B).

[Note: This is a potent recovery factor for an error in step F.17.a above because if the breakers are left open, the "closed" light (or the "open" light, for that matter) will not appear in the control room. For screening purposes, we assess the usual HEP of .1 for this recovery factor, assuming complete dependence for the human actions related to the two lights.]

3.3 Critical Steps in Procedure for Human Error #3:

"F.17.a.3) SBLC Injection Line Stop, 1C41-F008 (2C41-F008).

a) OPEN 1C41-F008 (2C41-F008) and LOCK.

b) RECORD position of 1C41-F008 (2C41-F008) on Attachment 1A(2A)."

[Note: Step 19 specifies that the SBLC Pump Flow Test will be performed after completion of the SBLC System Injection Test. The following step from LOS-SC-M1 provides a potent recovery factor for an error in F.17.a.3 above.]

"F.9. At panel 1H13-P603 (2H13-P603), CHECK the following and RECORD on Attachment 1A(2A).

a. Open light indication for 1C41-F008 (2C41-F008).

[Note: This is a potent recovery factor because the position of the manual valve is not changed during the Pump Flow Test. However, since this is a screening analysis, the usual HEP of .1 is assessed.]

4. Assumptions and Notes:

4.1 In none of the steps above do the related blanks in Attachment 1A(2A) call for second person verification.

4.2 It is assumed that there are no unrecovered errors in the written procedures and attachments. (This assumption is not critical; see Total-Failure HEP #5.)

4.3 Assumptions 1, 3, 4, 5, 7, and 8 from Total-Failure HEP #1 are relevant here.

4.4 Both squibs are tested during the same time period. If this assumption is incorrect, the assumption of complete dependence for

errors of omission for leaving disconnected explosive valves F004A and B and for failing to close breakers for MOVs F001A and B is not valid.

4.5 Checking for external leakage of the explosive valves provides no recovery factor for failing to reconnect the valves.

4.6 There may be other recovery factors in LOP-SC-02, which we do not have.

5. Pre-Accident Generic HRA Event Trees #2 and #3:

5.1 Pre-Accident Generic HRA Event Tree #2 (Figure A-6):

Operator omits or fails to connect fully an electrical connection, no other errors of commission are assessed, correct written procedures consisting of a long list (>10 items) to be used, and the record of the connection is to be made on a separate recording form.

5.2 Pre-Accident Generic HRA Event Tree #3 (Figure A-7):

Operator omits an item from a long list (>10 items), correct procedures to be used, and no record of the activity is made on a checklist or separate recording form.

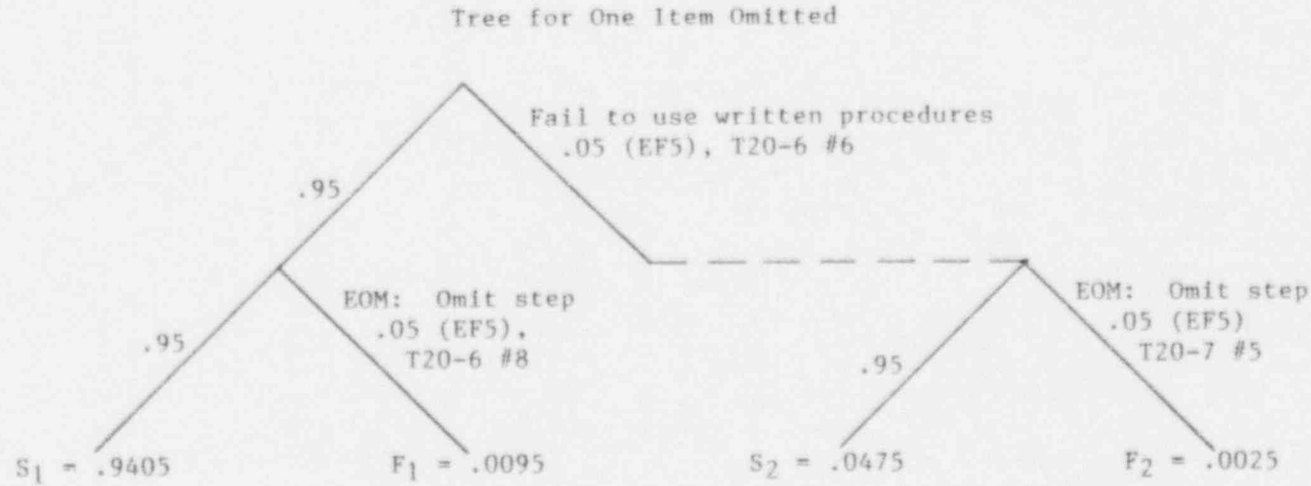
6. HEP Screening Estimates:

6.1 Human Error #1: Leave disconnected explosive valve F004A and or B (see 3.1 above).

6.1.1 Complete dependence (CD) is assessed for the error of omission (EOM) (T20-21 #5a), but zero dependence (ZD) (T20-21 #1a) is assessed for the error of commission (ECOM) of failing to reconnect <u>fully</u> the electrical cables to the two valves. (This error consists of initiating a connection of a cable to a valve, but, for some reason, a complete connection is not made.) For screening purposes, this ECOM is postulated, while selection errors are considered unimportant. It is presumed that the only possible selection error is one of reversal. If a reversal error is made between the two valves, it is assumed either that this error will be fully recovered or that it has no effect on the availability of either valve.

6.1.2 With the above screening assumptions, EOM is for <u>both</u> valves and ECOM is for <u>each</u> valve. Exclusive of recovery factors, and using the Pre-Accident Generic HRA Event Tree #2 (Figure A-6),

Figure A-6 Pre-Accident Generic HRA Event Tree #2



$S_T + F_T = .988 + .012 = 1.0.$ $F_T \approx .01$

Figure A-7 Pre-Accident Generic HRA Event Tree #3

$F_{EOM} = F_2 + F_4 + F_6 = .008675 \sim .009$ for <u>both</u> valves.

$F_{ECOM} = F_1 + F_3 + F_5 = .002974 \sim .003$ for <u>each</u> valve.

6.1.3 If failure is defined as either or both valves being left in an unavailable state (exclusive of recovery factors),

$F_T = .009 + .003 + .003 = .015$

If failure is defined as both valves being left in an unavailable state (exclusive of recovery factors),

$F_T = .009 + (.003)^2 \sim .009$

6.1.4 For screening purposes, a .1 HEP for recovery is assessed when a valid recovery factor exists. It is assumed that step F.1 in LOS-SC-M1 is such a recovery factor (see 3.1). Thus, the above two F_T terms are each multiplied by .1 and become .0015 and .0009, rounded to .002 and .001, respectively.

6.2 Human Error #2: Fail to close breakers for inlet MOVs F001A and/or B (see 3.2).

6.2.1 Complete dependence is assessed for EOM and no ECOM is assessed.

6.2.2 With this assumption, using Pre-Accident Generic HRA Event Tree #3 (Figure A-7), and exclusive of recovery factors,

$F_T = .01$ for either or both valves

6.2.3 For screening purposes, a .1 HEP for recovery is assessed, consisting of step F.9 in LOS-SC-M1 (see 3.2). Thus, the above F_T term is multiplied by .1 and becomes .001.

6.3 Human Error #3: Fail to open outlet maintenance manual valve F008 (see 3.3).

6.3.1 For screening purposes, it is assumed selection errors are possible as well as the nominal error of omission discussed earlier. Therefore, Pre-Accident Generic HRA Event Tree #1 is relevant, and the F_T is assessed as .02, exclusive of recovery factors.

6.3.2 For screening purposes, a .1 HEP for recovery is assessed, consisting of step F.9 in LOS-SC-M1. Thus, the above F_T is multiplied by .1 and becomes .002.

A.3 Total-Failure HEP #5 for Screening Pre-Accident HRA

1. Subject: Screening Analysis of the Repair of Valves 2C41-F004A or B, or Drain Valves 2C41-F312, F026, F308, and F024.

2. Critical Steps from Following Procedure: None, but it is assumed that a special (ad hoc) written procedure like step F.17.a.3 in LOS-SC-R1, Rev. 6, with Attachment 2A, would be prepared prior to the repair. Figure A-8 is a copy of this recording form.

2.1 "F.17 After the Explosive Valve has been replaced and the outage is cleared, RETURN the SBLC System to service as follows:

a. CLEAR the out-of-service on the following SBLC System components and position as follows:

3) SBLC Injection Line Stop, 1C41-F008 (2C41-F008).

a) OPEN 1C41-F008 (2C41-F008) and LOCK.

b) RECORD position of 1C41-F008 (2C41-F008) on Attachment 1A(2A)."

3. Assumptions and Notes:

3.1 No second operator verification, just as none is required in Attachment 2A for step 17.a.3.

3.2 An ad hoc restoration procedure will be prepared. Therefore, item #5 in T20-6 is relevant, in which an HEP of .01 is assessed for failure to use a valve change or restoration list, the operator depending instead on his memory. The implication of this .01 HEP for the estimated F_T is presented in paragraph 5.2 below.

3.3 Since this is a special restoration procedure, errors of omission (EOM) and errors of commission (ECOM) in writing it should be assessed. It is assumed that items 1 and 3 from T20-5 are appropriate, with a recovery factor by a second person per T20-22 #1. However, if the checker discovers an EOM, it is assumed that he or she will insure that there is no subsequent ECOM once the over-looked item is written. (This is the rational for S_3 in the HRA event tree in Figure A-9.)

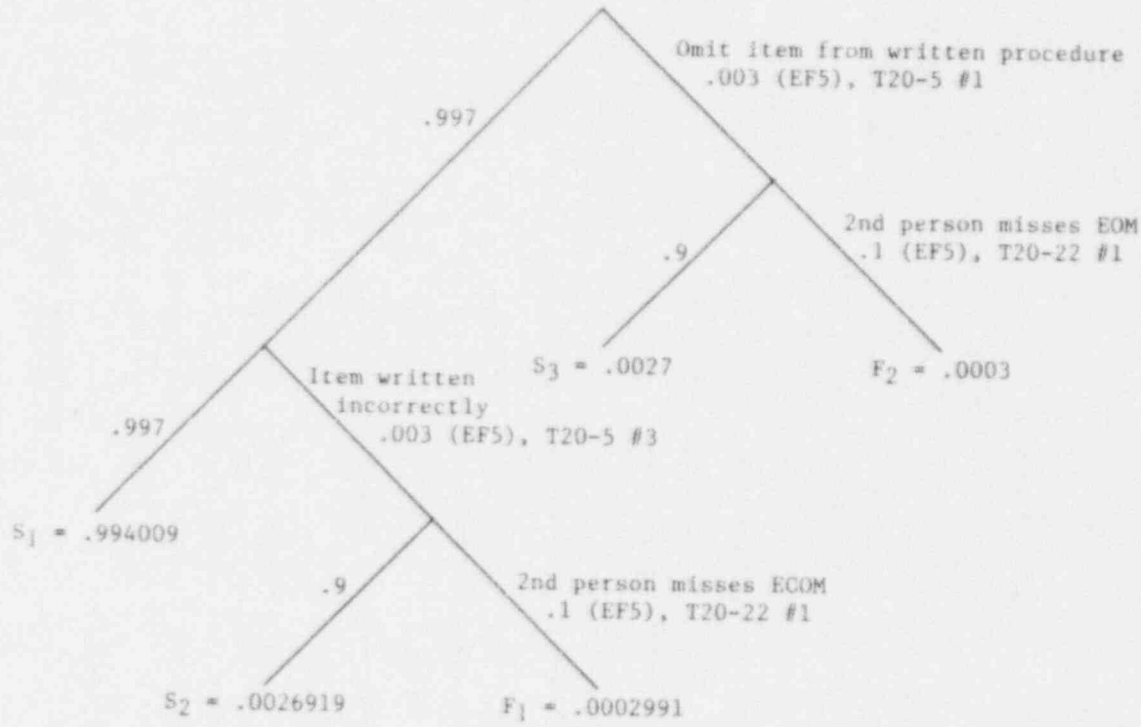
3.4 The writing errors pertain only to the written procedures, i.e., it is assumed that any errors in the recording form will be fully recoverable. If the operator is directed by the procedure to go to an item in the recording form, and if that item is missing or is incorrect, he or she should detect and correct these errors.

ATTACHMENT 2A

UNIT 2 SBLC INJECTION TEST SIGNOFF SHEET

PARAGRAPH NUMBER	DESCRIPTION/LIMITS	REQUIRED VALUE	OBSERVED VALUE	OPERATOR INITIALS
F.14	2C41-F031 position indicated at 2H13-P603	Indicated FULLY CLOSED		
F.15.a.1	2C41-F008, SBLC Injection Line Stop, position prior to unlocking.	LOCKED OPEN		
F.15.e.1	2C41-F003A, SBLC Pump Discharge Stop, position prior to unlocking.	LOCKED OPEN		
F.15.f.1	2C41-F003B, SBLC Pump Discharge Stop, position prior to unlocking.	LOCKED OPEN		
F.17.a.3.b	2C41-F008, SBLC Injection Line Stop, position after relocking.	LOCKED OPEN		
F.17.a.7.b	2C41-F003A, SBLC Pump Discharge Stop, position after relocking.	LOCKED OPEN		
F.17.a.8.b	2C41-F003B, SBLC Pump Discharge Stop, position after relocking.	LOCKED OPEN		
F.17.b	Explosive Valve, 2C41-F004A and 2C41-F004B Cables	CONNECTED TO VALVE		
F.17.c	SBLC System Lineup	SBLC SYSTEM LINED UP PER LOP-SC-02		

Figure A-8 Attachment 2A to LOS-SC-R1, Rev. 6



$S_T + F_T = .9994009 + .0005991 = 1.0.$ $F_T \approx .0006.$

Figure A-9 Pre-Accident Generic HRA Event Tree #4

3.5 Complete dependence (T20-21 #5a) is assumed for EOM for steps a) and b) in step F.17.a.3 above.

4. Pre-Accident Generic HRA Event Trees #4 and #5:

4.1 Pre-Accident Generic HRA Event Tree #4 (Figure A-9):

Operator omits an item from a special written procedure or makes an error of commission in writing the item, and a second person fails to catch either error.

4.2 Pre-Accident Generic HRA Event Tree #5 (Figure A-10):

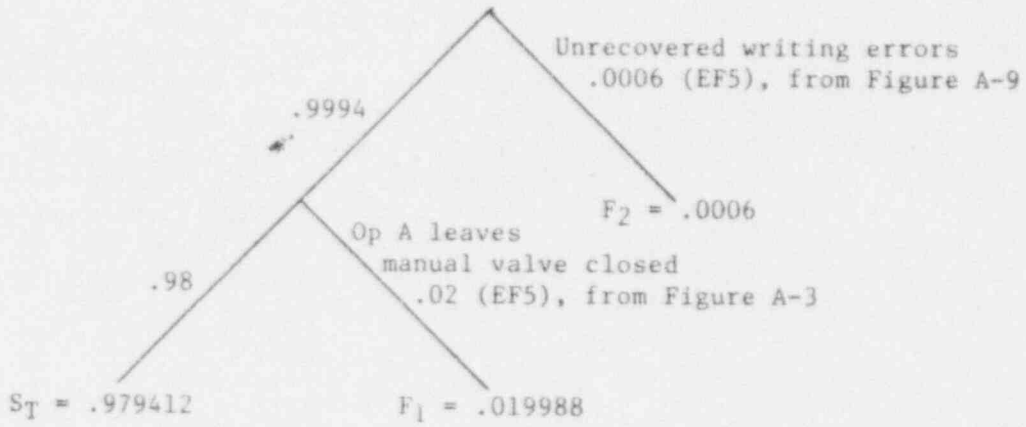
Operator fails to restore a locally-operated valve after valve repair, specially prepared (ad hoc) written procedures to be used, valve position to be written down on a separate recording form, unrecovered errors of omission and commission in the preparation of the ad hoc written procedures are possible, but any such errors on the recording form are assumed to be fully recoverable. (Note that this tree does not include recovery factors for the restoration failure, e.g., the use of a second person to check the first person's work. The tree does include recovery factors for preparation of special written procedures.)

5. HEP Screening Estimates:

5.1 Operator HEPs of .003 each for EOM and ECOM in writing ad hoc procedures are taken from items 1 and 3 of T20-5. These are multiplied by the recovery HEP of .1 (T20-22 #1) to provide the unrecovered writing HEPs of .0003 each for EOM and ECOM, as shown in Figure A-9.

5.2 HEP = .02 for leaving manual valve 2C41-F008 closed, assuming correct procedures used. The .02 comes from the same analysis used for Total-Failure HEP #1 (see Figure A-3). Substitution of a .01 probability of failure to use written procedures (T20-6 #5) in place of the .05 HEP used in Figure A-3 does not change the answer of .02 rounded. The HEP of .01 is for a valve change or restoration list, while the .05 is for the probability of failure to use written test or calibration procedures, and instead, relying on memory.

5.3 With no assumption about the correctness of the ad hoc procedures, the same HEP = .02 applies for the error in 5.2 above. See Figure A-10. Thus, the probability of incorrect ad hoc written procedures does not materially affect the overall probability of failure.



$S_T + F_T = .979412 + .020588 = 1.0.$ $F_T \approx .02$

Figure A-10 Pre-Accident Generic HRA Event Tree #5

APPENDIX B

LASALLE TEST AND MAINTENANCE PROCEDURE IDENTIFICATION

B.0 LASALLE TEST AND MAINTENANCE PROCEDURE IDENTIFICATION

B.1 Procedures With No Intersystem Dependencies

The following is a list of all test and maintenance procedures within the culled group for which no intersystem dependencies were found. These procedures were identified through review of the LaSalle test and maintenance procedure index.

B.1.1 Operating Surveillances (LOS)

LOS-AA-W1	LOS-AA-S2	LOS-AA-D1
LOS-AP-R1	LOS-DC-M1	LOS-DC-Q2
LOS-DC-Q3	LOS-DG-M1	LOS-DG-Q1
LOS-DG-SA1	LOS-FW-A1	LOS-HP-M1
LOS-HP-Q1	LOS-HP-R1	LOS-AA-Q1
LOS-LP-Q2	LOS-LO-Q3	LOS-LP-M1
LOS-MS-Q1	LOS-MS-R1	LOS-MR-R2
LOS-AA-R4	LOS-PC-M2	LOS-RH-M1
LOS-RH-Q1	LOS-RH-Q2	LOS-RH-Q3
LOS-SC-M1	LOS-SC-R1	LOS-SC-Q3
LOS-SC-R3	LOS-SC-R4	

B.1.2 Instrument Maintenance Surveillances (LIS)

LIS-CM-01	LIS-CM-03	LIS-CM-2041
LIS-CM-205	LIS-CM-404	LIS-CM-405
LIS-EH-03	LIS-FW-201	LIS-FW-401
LIS-HP-02	LIS-HP-04	LIS-HP-05
LIS-HP-06	LIS-HP-07	LIS-HP-08
LIS-HP-09	LIS-HP-401	LIS-MS-01
LIS-MS-02	LIS-MS-06	LIS-MS-204
LIS-MS-205	LIS-MS-404	LIS-MS-405
LIS-MB-10	LIS-NB-17	LIS-RR-05
LIS-SC-01	LIS-SC-02	LIS-SC-03

B.1.3 Tech Staff Surveillances (LTS)

LTS-100-3	LTS-100-4	LTS-100-22
LTS-100-34	LTS-100-35	LTS-100-36
LTS-100-43	LTS-100-44	LTS-100-45
LTS-900-2	LTS-900-3	LTS-900-4
LTS-900-9	LTS-900-12	

B.1.4 Electrical Maintenance Procedures (LEP)

LEP-MO-109

B.1.5 Electrical Maintenance Surveillances (LES)

LES-DC-102	LES-DC-104	LES-DC-105
LES-DC-107	LES-FW-01	LES-HP-02
LES-MS-02	LES-MS-03	LES-NB-01
LES-PC-08	LES-RI-01	LES-RP-03
LES-RR-01		

B.1.6 Mechanical Maintenance Procedures (LMP)

LMP-MS-03	LMP-MS-04	LMP-TG-01

B.1.7 Instrument Maintenance Procedures (LIP)

LIP-EH-01	LIP-FW-01	LIP-FW-02
LIP-FW-05	LIP-FW-08	LIP-FW-607
LIP-GM-02	LIP-MS-01	LIP-NB-06
LIP-SC-01	LIP-SC-02	LIP-TG-01

B.1.8 Operating Procedures (LOP)

LOP-AP-05	LOP-AP-10	LOP-AP-11
LOP-AP-12	LOP-AP-16	LOP-AP-17
LOP-AP-18	LOP-AP-19	LOP-AP-22
LOP-CO-01E	LOP-CX-101	LOP-CS-02E
LOP-DC-07	LOP-DC-01T	LOP-DG-01
LOP-DG-02	LOP-DG-03	LOP-DG-04
LOP-DG-05	LOP-DG-06	LOP-DG-07
LOP-DG-08	LOP-DG-09	LOP-DG-10
LOP-DG-11	LOP-DG-13	LOP-DG-04E
LOP-DG-05E	LOP-DG-09E	LOP-DG-18E
LOP-DG-04M	LOP-DG-05M	LOP-DG-09M
LOP-DG-10M	LOP-DM-01M	LOP-DO-02
LOP-DG-02E	LOP-FP-02	LOP-FP-01E
LOP-FW-02E	LOP-FW-02M	LOP-FW-04M
LOP-FW-06M	LOP-HP-01	LOP-HP-03
LOP-HP-04	LOP-HP-05	LOP-LP-01
LOP-LP-02	LOP-LP-03	LOP-LP-02M
LOP-LP-02E	LOP-MS-03	LOP-MS-06
LOP-MS-02E	LOP-MS-04E	LOP-MS-02M
LOP-MS-04M	LOP-MS-06M	LOP-RH-02
LOP-RH-03	LOP-RH-04	LOP-RH-05
LOP-RH-06	LOP-RH-07	LOP-RH-08
LOP-RH-10	LOP-RH-11	LOP-RH-12
LOP-RH-13	LOP-RH-14	LOP-RH-15
LOP-RH-16	LOP-RH-18	LOP-RH-03E
LOP-RH-04E	LOP-RH-03M	LOP-RH-04M
LOP-RH-05M	LOP-RH-06M	LOP-RX-02E
LOP-SC-07	LOP-SC-01E	LOP-SC-02E
LOP-SC-01M	LOP-SC-02M	LOP-VD-02E

LOP-VD-04E LOP-VE-01 LOP-VE-03
LOP-VE-04

B.1.9 Mechanical Maintenance Surveillances (LMS)

LMS-DG-01

B.1.10 Tech Staff Procedures (LTP)

LTP-300-11 LTP-800-13

B.2 Procedures with Intersystem Dependencies

The following is a list of procedures where intersystem dependencies are identified. For each procedure, a brief summary of the intersystem dependency is included.

B.2.1 Operating Procedure (LOP)

(1) LOP-AP-01, Restoring the System Auxiliary Transformer SAT 242 to Service with Unit Two in Shutdown. Breakers ACB 2512, ACB 2522, ACB 2412, ACB 2422, and ACB 2432 are racked in. 345 KV ring breakers OCB 1-6 and OCB 4 are opened. Fuses are installed for 6.0 KV bus 252. Diesel generators 0 and 2A are shutdown and their output breakers are open.

(2) LOP-AP-02, Restoring the System Auxiliary Transformer to Service During Unit Operation. Breakers ACB 2432, ACB 2422, ACB 2412, ACB 2512, and ACB 2522 are racked in. 345 KV ring breakers OCB 1-6 and OCB 4-6 are opened and then closed. Power is transferred on buses 252, 241-4, 242-4, and 242-X. The HPCS battery 223 is transferred to its normal source of power. Diesel generator 2B is returned to automatic.

(3) LOP-AP-03, Racking in a 6900 Volt or 4160 Volt Manually Operated Air Circuit Breaker to "Test" or "connected" Position. This procedure applies to all of these breaker types, on a plant encompassing basis, with the exception of switchgear 243 and those at the Lake Screen House.

(4) LOP-AP-04, Racking in a 4160 Volt Motor Operated Air Circuit Breaker. This procedure has the identical dependencies of LOP-AP-03.

(5) LOP-AP-06, Returning a 480 Volt Transformer to Service. This is a plant encompassing procedure for all 480 V transformers.

(6) LOP-AP-07, Removing the System Auxiliary Transformer from Service During Unit Operation. This procedure has the same dependencies as LOP-AP-02.

(7) LOP-AP-08, Removing System Auxiliary Transformer SAT 242 from Service with Unit 2 in Shutdown. Breakers ACB 2411, ACB 2421, ACB 2511, and ACB 2521 are racked in. Breakers ACB 2512, ACB 2522, ACB 2412, ACB 2422, and ACB 2432 are racked out.

(8) LOP-AP-09, Removing a 4160 Volt Vertical Type Motor Operated Circuit Breaker from Test. This is a plant encompassing procedure for all of these types of circuit breakers.

(9) LOP-AP-14, Transfer of 6.0 KV or 4.16 KV Bus Power Supply Between the System and Unit Auxiliary Transformers. This procedure affects all 6.9 KV and 4.16 KV power supplies for the unit auxiliary transformers.

(10) LOP-AP-20, 480 Volt Air Circuit Breaker Operation. This is a plant encompassing procedure for all of these types of breakers.

(11) LOP-AP-21, Motor Operated Valves. This is a plant encompassing procedure for fault determination in all motor operated valves.

(12) LOP-AP-02E, Pre-Startup Electrical Lineup. This procedure verifies power supplies and breakers positions at thirty switch gears and thirty-five motor control centers.

(13) LOP-DC-01, Energizing, Startup, and Shutdown of a Battery Charger. This is a plant encompassing procedure for all batteries.

(14) LOP-DC-02, Changing Modes of Operation in the DC Electrical System. This is a plant encompassing procedure for all 250 VDC and 125 VDC distribution panels.

(15) LOP-DC-03, 250 VDC System Ground Location and Isolation. All 250 VDC loads have the potential to be secured and then returned to service.

(16) LOP-DC-04, 125 VDC System Division I Ground Location and Isolation. This procedure has the same criteria as LOP-DC-03.

(17) LOP-DC-05, 125 VDC System Division 2 Ground Location and Isolation. This procedure has the same criteria as LOP-DC-03.

(18) LOP-DC-06, 125 VDC System Division 3 Ground Location and Isolation. This procedure has the same criteria as LOP-DC-03.

(19) LOP-DG-12, Fill and Vent the Standby Diesel Generator "0" ODG01K Cooling System. This procedure affects the LPCS pump motor cooler inlet and outlet pressure instrument root stop.

(20) LOP-DG-08M, Diesel Generator Cooling Water. This procedure checks LPCS pump cooler indications and valves.

(21) LOP-DC-07E, Division 1 125 VDC. This is an electrical checklist of all loads on Division 1.

(22) LOP-DC-08E, Division 2 125 VDC. This procedure has the same criteria as LOP-DC-07E.

(23) LOP-DW-02M, Drywell for Manual Valves. This procedure checks valve positions of the RCIC, LPCI, RHR, SBLC, and HPCS systems.

(24) LOP-RH-01, Filling and Venting the Residual Heat Removal System (RHR). LPCI piping is also filled. RCIC valves are manipulated.

(25) LOP-RH-09, Steam Condensing Startup Operation. Both the RHR and the RCIC systems are manipulated.

(26) LOP-RH-17, Alternate Shutdown Cooling. The RHR, LPCS, and RCIC systems are manipulated.

(27) LOP-RH-19, Unit 2 Steam Condensing Startup and Operation. This procedure has the same criteria as LOP-RH-09.

B.2.2 Instrument Maintenance Surveillances (LIS)

(1) LIS-PC-203, Unit 2 High Drywell Pressure LPCS Initiation, RHR (LPCI mode) Initiation, ADS Permissive, and RCIC Calibration. Logic setpoints are calibrated on all the afore-mentioned systems.

B.2.3 Electrical Maintenance Surveillances (LES)

(1) LES-AP-02, Setting and Testing of General Electric Over-current Protective Devices (480 VAC). This is a plant encompassing procedure for this breaker type.

(2) LES-DC-101, 24, 125, and 250 Volt Battery Inspection. This is a plant encompassing procedure for these battery types.

(3) LES-GM-223, Southern Division A.O.D. Meter Calibrations. This procedure calibrates many plant wide meters.

B.2.4 Operating Surveillances (LOS)

(1) LOS-AA-S1, Shiftly Surveillance. This procedure checks indications on many systems.

(2) LOS-DC-Q2, Charging Requirements and Battery Readings for the Safety Related 250 VDC and 125 VDC Batteries. This is a plant encompassing procedure for all 125 VDC and 250 VDC batteries.

(3) LOS-RI-Q1, RCIC Valve Inservice Test for Operating, Start-up, and Hot Shutdown Conditions. Main and turbine feedwater trips are bypassed.

(4) LOS-RI-R1, Reactor Core Isolation Cooling Turbine Over-speed Test. The suppression pool cooling mode of RHR must be in operation.

Distribution

James Abel
Commonwealth Edison Co.
35 1st National West
Chicago, IL 60690

Kiyoharu Abe
Department of Reactor Safety
Research
Nuclear Safety Research Center
Tokai Research Establishment
JAERI
Tokai-mura, Naga-gun
Ibaraki-ken,
JAPAN

Bharat B. Agrawal
USNRC-RES/PRAB
MS: NLS-372

J. Alman
Commonwealth Edison Co.
LaSalle County Station
RR1, Box 220
2601 North 21st Rd.
Marsielles, IL 61341

George Apostolakis
UCLA
Boelter Hall, Room 5532
Los Angeles, CA 90024

Vladimar Asmolov
Head, Nuclear Safety Department
I. V. Kurchatov Institute
of Atomic Energy
Moscow, 123182
U.S.S.R.

Patrick W. Baranowsky
USNRC-AEOD/TPAB
MS: 9112

Robert A. Bari
Brookhaven National Laboratories
Building 130
Upton, NY 11973

Richard J. Barrett
USNRC-NRR/PD3-2
MS: 13 D1

William D. Beckner
USNRC-NRR/PRAB
MS: 10 E4

Dennis Bley
Pickard, Lowe & Garrick
2260 University Drive
Newport Beach, CA 92660

Gary Boyd
Safety & Reliability Optimization
Services
9724 Kingston Pike, Suite 102
Knoxville, TN 37922

Robert J. Budnitz
Future Resources Associates
734 Alameda
Berkeley, CA 94707

Gary R. Burdick
USNRC-RES/RPSIB
MS: NLS-314

Arthur J. Buslik
USNRC-RES/PRAB
MS: NLS-372

Annick Carnino
Electricite de France
32 Rue de Monceau 8EME
Paris, F5008
FRANCE

S. Chakraborty
Radiation Protection Section
Div. De La Securite Des Inst. Nuc.
5303 Wurenlingen
SWITZERLAND

Michael Corradini
University of Wisconsin
1500 Johnson Drive
Madison, WI 53706

George Crane
1570 E. Hobble Creek Dr.
Springville, Utah 84663

Mark A. Cunningham
USNRC-RES/PRAB
MS: NLS-372

G. Diederick
Commonwealth Edison Co.
LaSalle County Station
RR1, Box 220
2601 North 21st Rd.
Marsielles, IL 61341

Mary T. Drouin
Science Applications International
Corporation
2109 Air Park Road S.E.
Albuquerque, NM 87106

Adel A. El-Bassioni
USNRC-NRR/PRAB
MS: 10 E4

S. A. Eide
Energy International Inc.
Idaho Falls, Idaho

Robert Elliott
USNRC-NRR/PD3-2
MS: 13 D1

Farouk Eltawila
USNRC-RES/AEB
MS: NLN-344

John H. Flack
USNRC-RES/SAIB
MS: NLS-324

Karl Fleming
Pickard, Lowe & Garrick
2260 University Drive
Newport Beach, CA 92660

James C. Glynn
USNRC-RES/PRAB
MS: NLS-372

T. Hammerich
Commonwealth Edison Co.
LaSalle County Station
RR1, Box 220
2601 North 21st Rd.
Marsielles, IL 61341

Robert A. Hasse
USNRC-RGN-III
MS: RIII

Sharif Heger
UNM Chemical and Nuclear
Engineering Department
Farris Engineering
Room 209
Albuquerque, NM 87131

P. M. Herttrich
Federal Ministry for the
Environment, Preservation of
Nature and Reactor Safety
Husarenstrasse 30
Postfach 120629
D-5300 Bonn 1
FEDERAL REPUBLIC OF GERMANY

S. Hirschberg
Department of Nuclear Energy
Division of Nuclear Safety
International Atomic Energy Agency
Wagramerstrasse 5, P.O. Box 100
A-1400 Vienna
AUSTRIA

M. Dean Houston
USNRC-ACRS
MS: P-315

Alejandro Huerta-Bahena
National Commission on Nuclear
Safety and Safeguards (CNSNS)
Insurgentes Sur N. 1776
C. P. 04230 Mexico, D. F.
MEXICO

Peter Humphreys
US Atomic Energy Authority
Wigshaw Lane, Culcheth
Warrington, Cheshire
UNITED KINGDOM, WA3 4NE

W. Huntington
Commonwealth Edison Co.
LaSalle County Station
RR1, Box 220
2601 North 21st Rd.
Marsielles, Il 61341

Brian Ivee
UNC Nuclear Industries
P. O. Box 490
Richland, WA 99352

William Kastenberg
UCLA
Boelter Hall, Room 5532
Los Angeles, CA 90024

George Klopp [10]
Commonwealth Edison Company
P.O. Box 767, Room 35W
Chicago, IL 60690

Alan Kolaczkowski
Science Applications Int. Corp.
2109 Air Park Rd. SE
Albuquerque, NM 87106

Jim Kolanowski
Commonwealth Edison Co.
35 1st National West
Chicago, IL 60690

S. Kondo
Department of Nuclear Engineering
Facility of Engineering
University of Tokyo
3-1, Hongo 7, Bunkyo-ku
Tokyo
JAPAN

Jose A. Lantaron
Cosejo de Suguridad Nuclear
Sub. Analisis y Evaluaciones
Justo Dorado, 11
28040 Madrid
SPAIN

Josette Larchier-Boulanger
Electricte de France
Direction des Etudes Et Recherches
30, Rue de Conde
65006 Paris
FRANCE

Librarian
NUMARC/USCEA
1776 I Street NW, Suite 400
Washington, DC 80006

Bo Liwnang
IAEA A-1400
Swedish Nuclear Power Inspectorate
P.O. Box 27106
S-102 52 Stockholm
SWEDEN

Peter Lohnberg
Expresswork International, Inc.
1740 Technology Drive
San Jose, CA 95110

Steven M. Long
USNRC-NRR/PRAB
MS: 10 E4

Herbert Massin
Commonwealth Edison Co.
35 1st National West
Chicago, IL 60690

Andrew S. McClymont
IT-Delian Corporation
1340 Saratoga-Sunnyvale Rd.
Suite 206
San Jose, CA 95129

Jose I. Calvo Molins
Head, Division of P.S.A. and Human Factors
Consejo De Seguridad Nuclear
Justo Dorado, 11
28040 Madrid
SPAIN

Joseph A. Murphy
USNRC-RES/DSR
MS: NLS-007

Kenneth G. Murphy, Jr.
US Department of Energy
19901 Germantown Rd.
Germantown, MD 20545

Robert L. Palla, Jr.
USNRC-NRR/PRAB
MS: 10 E4

Gareth Parry
NUS Corporation
910 Clopper Rd.
Gaithersburg, MD 20878

G. Petrangeli
ENEA Nuclear Energy ALT Disp
Via V. Brancati, 48
00144 Rome
ITALY

Ing. Jose Antonio Becerra Perez
Comision Nacional De Seguridad
Nuclear Y Salvaguardias
Insurgentes Sur 1806
01030 Mexico, D. F.
MEXICO

William T. Pratt
Brookhaven National Laboratory
Building 130
Upton, NY 11973

William Raisin
NUMARC
1726 M. St. NW
Suite 904
Washington, DC 20036

D. M. Rasmuson
USNRC-RES/SAIB
MS: NLS-372

John N. Ridgely
USNRC-RES/SAIB
MS: NLS-324

Richard C. Robinson Jr.
USNRC-RES/PRAB
MS: NLS-372

Denwood F. Ross
USNRC-AEOD
MS: 3701

Takashi Sato
Deputy Manager
Nuclear Safety Engineering Section
Reactor Design Engineering Dept.
Nuclear Energy Group
Toshiba Corporation
Isogo Engineering Center
8, Shinsugita-cho, Isogo-ku,
Yokohama 235,
JAPAN

Martin Sattison
Idaho National Engineering Lab.
P. O. Box 1625
Idaho Falls, ID 83415

Louis M. Shotkin
USNRC-RES/RPSB
MS: NLN-353

Desmond Stack
Los Alamos National Laboratory
Group Q-6, Mail Stop K556
Los Alamos, NM 87545

Alan Swain
712 Sundown Pl. SE
Albuquerque, NM 87108

T. G. Theofanous
University of California, S. B.
Department of Chemical and Nuclear
Engineering
Santa Barbara, CA 93106

Harold VanderMolen [10]
USNRC-RES/PRAB
MS: NLS-372

Magiel F. Versteeg
Inspector Reactor Safety
Nuclear Safety Department
Directorate-General of Labour
Ministry of Social Affairs and Employment
P.O. Box 90804
2509 LV Den Haag
Anna van Hannoverstraat 4

Edward Warman
Stone & Webster Engineering Corp.
P.O. Box 2325
Boston, MA 02107

Wolfgang Werner
Gesellschaft Fur Reaktorsicherheit
Forschungsgelande
D-8046 Garching
FEDERAL REPUBLIC OF GERMANY

7141 Technical Library [5]
7151 Technical Publications [1]
6321 T. A. Wheeler
6400 N. R. Ortiz
6405 D. A. Dahlgren
6411 D. D. Carlson
6411 D. M. Kunsman
6411 R. J. Breeding
6411 K. J. Maloney
6412 A. L. Camp
6412 S. E. Dingman
6412 B. D. Staple

6412 G. D. Wyss
6412 A. C. Payne, Jr. [25]
6412 D. W. Whitehead
6413 F. T. Harper
6413 T. D. Brown
6449 M. P. Bohn
6449 J. A. Lambright
8523-2 Central Technical Files

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-4832
SAND92-0537
Vol. 5

2 TITLE AND SUBTITLE

Analysis of the LaSalle Unit 2 Nuclear Power Plant: Risk Methods Integration and Evaluation Program
Parameter Estimation Analysis and Screening Human Reliability Analysis

3 DATE REPORT PUBLISHED

MONTH: March
YEAR: 1993

4 FIN OR GRANT NUMBER

A1386

5 AUTHOR(S)

T. A. Wheeler, A. D. Swain, J. A. Lambright, A. C. Payne, Jr.

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.)

Sandia National Laboratories
P. O. Box 5800
Albuquerque, NM 87185

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

Division of Safety Issue Resolution
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

10 SUPPLEMENTARY NOTES

11 ABSTRACT (200 words or less)

This volume describes the methodologies used in the data analysis, the screening human error analysis, and the common mode human error analysis performed in support of the LaSalle PRA. Selected results are presented in this volume. The remainder of the results are presented in other volumes of this report where they are actually used. The data review process used in the determination of the data used for the initial screening analysis is described and the final screening data base is given. The final data selection process is described and the final data distributions are presented. The actual implementation of the data base for the integrated accident sequence quantification is described in Volume 2 of this report on Integrated Quantification and Uncertainty Analysis. Several new methods developed for use in analyzing both pre- and post- accident human errors for the initial screening analysis are described. Most of the actual results are given in other volumes of this report under the appropriate sub-analysis descriptions. A method for determining procedural common mode analysis is described and the results presented.

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

PRA
RMIEP
LaSalle
Level I

13 AVAILABILITY STATEMENT

Unlimited

14 SECURITY CLASSIFICATION

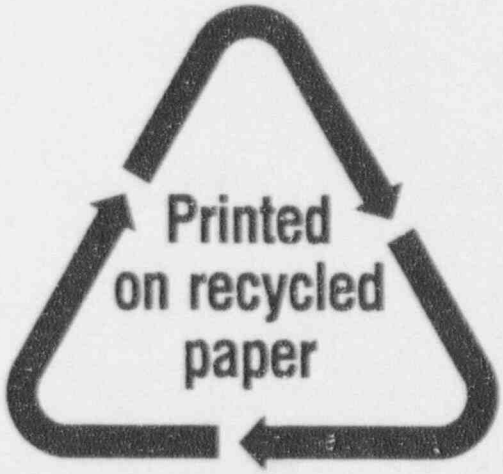
(This Page)
Unclassified

(This Report)
Unclassified

15 NUMBER OF PAGES

16 PRICE

NRC FORM 335 (2-89)



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001