NUREG
August 2001
INEEL/EXT-01-01166

Review of Findings for Human Error Contribution to Risk in Operating Events

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

NUREG
August 2001
INEEL/EXT-01-01166

Review of Findings for Human Error Contribution to Risk in Operating Events

Manuscript Completed: August 2001
Date Published:

Prepared by:
David I. Gertman, Principal Investigator
Bruce P. Hallbert, Program Manager
Mark W. Parrish
Martin B Sattision
Doug Brownson
James P. Tortorelli

Idaho National Engineering and Environmental Laboratory
Bechtel BWXT Idaho, LLC
Idaho Falls, Idaho 83415

NRC Program Managers
Eugene A. Trager
J. J. Persensky

Prepared for
Office of Nuclear Regulatory Research
Division of Systems Analysis and Regulatory Effectiveness
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC Job Code E8238

ABSTRACT

This report presents the findings of a study of the contributions of human performance to risk in operating events at commercial nuclear power plants. The Nuclear Regulatory Commission (NRC) Accident Sequence Precursor (ASP) Program and the Human Performance Events Database (HPED) were used to identify safety significant events in which human performance was a major contributor to risk. Conditional core damage probabilities (CCDPs) were calculated for these events using Systems Analysis Programs for Hands-on Integrated Reliability Evaluation (SAPHIRE) software and Standardized Plant Analysis Risk (SPAR) models.

Forty-eight events described in licensee event reports and augmented inspection team reports were reviewed. Human performance did not play a role in 11 of the events, so they were excluded from the sample. The remaining 37 events were qualitatively analyzed. Twenty-three of these 37 events were also analyzed using SPAR models and methods. Fourteen events were excluded from the SPAR analyses because they involved operating modes or conditions outside the scope of the SPAR models.

The results showed that human performance contributed significantly to analyzed events. Two hundred and seventy human errors were identified in the events reviewed and multiple human errors were involved in every event. Latent errors (i.e., errors committed prior to the event whose effects are not discovered until an event occurs) were present four times more often than were active errors (i.e., those occurring during event response). The latent errors included failures to correct known problems and errors committed during design, maintenance, and operations activities. The results of this study indicate that multiple errors in events contribute to the probabilistic risk assessment (PRA) basic events present in SPAR models and that the underlying models of dependency in HRA may warrant further attention.

CONTENTS

APPENDICES

LIST OF TABLES

EXECUTIVE SUMMARY

To better understand how human performance influences the risk associated with nuclear power plant operations, the U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES) requested the Idaho National Engineering and Environmental Laboratory (INEEL) to identify and characterize the influences of human performance in significant operating events. The INEEL used the Accident Sequence Precursor (ASP) program to identify events associated with high-risk sequences and the Standardized Plant Analysis Risk (SPAR) models to calculate measures of risk associated with human performance in those sequences.

Analysis results suggest a number of findings regarding the influence of human performance on the sample of significant operating events analyzed. The following six findings were considered to be the most important to probabilistic risk assessment (PRA) by the analysis team.

1. Human error contributed significantly to risk in nearly all events analyzed. Forty-one percent of events involved partial or complete loss of either onsite or offsite power, twenty-two percent involved loss of Emergency Core Cooling Systems (ECCS) and nineteen percent involved loss of feedwater. The increase in event risk for the operating events studied varies from 1.0E-6 to 1.0E-3 over the nominal core damage probability (CDP), which ranged from 1.3E-5 to 1.2E-4. The average human error contribution to the change in risk was 62%.

2. Latent errors were present in every event analyzed and were more predominant than active errors by a ratio of 4 to 1. Latent errors were noted in all facets of performance studied, including operations, design and design change work practices, maintenance practices and maintenance work controls, procedures and procedure development, corrective action program, and management supervision. The degree of latent error involvement in risk-significant operating events warrants attention. A study of the contribution of latent errors to the important basic events in models of plant risk would provide useful information especially in cases where the cause of the failure is important. This would help to focus resources on plant programs that are important contributors to plant risk.

3. Without exception, the operating events analyzed included multiple contributing factors. On the average, the 37 events contained 4 or more human errors in combination with hardware failures. Fifty percent of events contained five or more errors. Many events contained between six and eight human errors.

4. Human errors can result in the failure or increased likelihood of failure of risk-significant equipment. For a sample of ten events with the highest event importance, human error was determined to contribute to component failure. There were three events where a single human error contributed to a single PRA basic event, and seven events where multiple human errors contributed to multiple PRA basic events. Dependency between maintenance and design errors, and dependency between preceding and subsequent component failures in several event sequences suggests that the issue of the representation of dependency in human reliability analysis (HRA) needs to be given detailed consideration and failure rates for dependency determined.

5. Design and design change work practice errors were present in 81% of events, maintenance practices and maintenance work control errors were present in 76% of events, and operations errors were present in 54% of events. Additionally, more maintenance and operations errors mapped to basic events in the PRA model than did design and design change errors.

6. Forty-one percent of the analyzed events demonstrated evidence of failure to monitor, observe, or otherwise respond to negative trends, industry notices, or design problems. This suggests that inadequacies in licensee corrective action programs may play an important role in influencing

operating events. Indicators for determining when these processes are flawed, and what impacts on safety and performance may be expected, are recommended.

Areas for Potential Enhancement of HRA

This study has identified several areas for potential enhancements to HRA. They were characterized by the analysis team and are presented below for future consideration.

1. A method for using human performance data from operating events to support HRA should be considered. Updates to human error probability (HEP) reference values and distributions based upon operating experience would be a significant improvement for HRA.
2. HRA applications can be directed toward characterizing latent errors and a portion of work process variables present in events. Guidelines on how this can be integrated with existing fault tree and event tree models, including level of HRA analysis, should be developed as part of the HRA process.
3. Data on activities related to maintenance, surveillance, test, calibration, installation, and corrective action prioritization and processing would provide a technical basis that could be used in conjunction with the analysis of operating events for assessing the root causes of equipment failures and for potential recovery actions.
4. The mechanisms by which small, multiple errors impact risk and the linkages by which they combine should be better understood. After an initial human error, dependency calculation methods often increase subsequent HEP estimates. However, many small errors are often not considered or are discarded after the screening analysis. Often these small, multiple errors cross systems and components, but do not become important until the occurrence of the initiating event.
5. The percentage of hardware unavailability due to human error as opposed to random hardware failures is not known. If this were determined by review of plant specific data then the risk reduction associated with increased human reliability in these areas could be better approximated.

ACRONYMS

ACRS	Advisory Committee on Reactor Safety
AFW	auxiliary feedwater (system)
AIT	Augmented Inspection Team
ANO	ANO
ASEP	Accident Sequence Evaluation Program
ASP	Accident Sequence Precursor
ATHEANA	A Technique for Human Event Analysis
B&W	Babcock and Wilcox
BWR	boiling water reactor
CAHR	Connectionism Approach for Assessing the Reliability of Human Actions
CCDF	conditional core damage frequency
CCDP	conditional core damage probability
CCDPHE	Portion of CCDP due to human error
CDF	core damage frequency
CDP	core damage probability
COSIMO	Cognitive Model for Simulation of Operator's Behavior
CR	control room
CREAM	Comprehensive Reliability Analysis Method
CRIEPI	Central Research Institute of Electric Power Industry (Japan)
CW	circulating water
DG	diesel generator
DGCWP	diesel generator cooling water pump
ECCS	emergency core cooling system
EDG	emergency diesel generator
EFW	emergency feedwater (system)
EHC	electro-hydraulic control system
EMRV	electro-mechanical relief valve
ENEL	Italian Research Institute
ENS	emergency notification system
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
ERAT	emergency reserve auxiliary transformer
ESFAS	engineered safety features actuation system
ESWS	essential service water system
FRV	feedwater regulating valve
HEART	Human Error Analysis and Reduction Technique
HEP	human error probability
HI	human interaction
HMI	human machine interface
HPCI	high pressure coolant injection
HPED	Human Performance Events Database
HPI	high pressure (safety) injection
HRA	human reliability analysis
HVAC	heating, ventilation, and air conditioning
I&C	instrumentation and control

IE	initiating event
IIT	Incident Investigation Team
INEEL	Idaho National Engineering and Environmental Laboratory
INPO	Institute of Nuclear Power Operations
IPE	Individual Plant Examination
ISPRA	Institute for Systems Engineering and Informatics (Research Center, Italy)
JAERI	Japanese Atomic Energy Research Institute
LCO	limiting conditions for operations
LDST	letdown storage tank
LER	Licensee Event Report
LLOCA	large loss of coolant accident
LOCA	loss of coolant accident
LOOP	loss of offsite power
LTOP	low temperature over-pressure
MCC	motor control center
MERMOS	French safety analysis stressing the human factors safety mission
MFB	main feed breakers
MFW	main feedwater
MG	motor generator
MLOCA	medium loss of coolant accident
MOV	motor operated valve
MSIV	main steam isolation valve
MSSV	main steam safety valve
NEA	Nuclear Energy Agency
NOUE	notification of unusual event
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
NSS	nuclear shift supervisor
NUREG	Nuclear Regulatory Commission Report
OECD	Organization for Economic Cooperation and Development
ORE	operator reliability experiments
ORNL	Oak Ridge National Laboratory
PCIS	primary containment isolation system
PCIV	primary containment isolation valve
PCS	primary coolant system
PHP	Program on Human Performance
PORV	power operated relief valve
PRA	probabilistic risk assessment
PSA	probabilistic safety analysis
PSF	performance shaping factor
psia	pounds per square inch (atmospheric)
psid	pounds per square inch (differential)
psig	pounds per square inch (gauge)
PWR	pressurized water reactor
QA	quality assurance
RAS	recirculation actuation signal

RCIC	reactor core isolation cooling
RCP	reactor coolant pump
RCS	reactor coolant system
RES	Office of Nuclear Regulatory Research
RFI	risk factor increase
RHR	residual heat removal
RO	reactor operator
RPS	reactor protection system
RT	radiographic testing
RVLIS	reactor vessel level indication system
RWST	reactor water storage tank
RWT	refueling water tank
SAPHIRE	Systems Analysis Programs for Hands-on Integrated Reliability Evaluations
SAT	station auxiliary transformer
SBO	station blackout
SCRAM	safety critical reactor axe man
SCSS	Sequence Coding and Search System
SG	steam generator
SGTR	steam generator tube rupture
SHARP	systematic human action reliability procedure
SI	safety injection
SLIM	Success Likelihood Index Method
SLOCA	small loss-of-coolant accident
SNSS	senior nuclear shift supervisor
SPAR	Standardized Plant Analysis Risk
SPDS	safety parameter display system
SRO	senior reactor operator
SRV	safety relief valve
SS	system safety
STA	shift technical advisor
T_{ave}	average temperature
TDAFW	turbine driven auxiliary feedwater
THERP	Technique for Human Error Rate Prediction
TRANS	transient
TS	technical specification
UAT	unit auxiliary transformer
UST	unit service transformer
UT	ultrasonic testing
VAR	volt-ampere reactive
VVER	water-water energy reaction type PWR plant

1. INTRODUCTION AND BACKGROUND

The purpose of this report is to describe how human performance has affected recent operating events in commercial nuclear power plants and the root causes of that performance. Selected events were evaluated to determine the impact of human performance on those events. The work is intended to support the technical basis for identifying and prioritizing human performance research and to highlight the potential use of event analysis to better understand and identify the context[1] for human error

The present study also supports Task 1 objectives of the Nuclear Regulatory Commission Human Reliability Analysis (HRA) Research Program to: provide data to support quantification of failure probabilities, support and improve existing HRA models, and to further define HRA data needs.

The approach selected to identify the contribution of human performance to significant events was to analyze ASP events that had a calculated conditional core damage probability (CCDP) of 1.0E-5 or greater, in which human performance was an important contributing factor. Details regarding event selection are described in Section 2.

Because this study focuses on the human contribution to increased risk as observed in operating events, there is no consideration given to the positive impact of human performance on nuclear power plant risk. This does not imply that human performance has no positive impact, indeed, quite the opposite is true. Every event analyzed in this study was successfully terminated by actions of the operating crews.

1.1 Key Terms and Definitions

The following are definitions as used in this report.

Active Error – active errors are those that result in initiating events, or those that occur as a post-initiator response to an initiating event.

Basic Event – refers to the lowest level of component failure mode modeled in the PRA and can include human actions, as well as hardware unavailabilities and failures.

CCDP – conditional core damage probability. The core damage probability for a nuclear power plant given a set of component failures and human errors as observed in an operational event.

CDP – core damage probability. The likelihood of a nuclear power plant experiencing core damage over a given period of time based on the nominal core damage frequency (CDF). This is the base case for comparison to the CCDP in event assessment.

Event – operating event analyzed in the NRC ASP Program and used in this study.

Failure – the inability of a component or human to perform its functions as required by a probabilistic risk assessment (PRA) model. Failures are generally modeled as individual and independent basic events in a PRA.

Human error categories – represent the consolidation of error subcategories possessing a common theme. In the present study, six categories were identified: operations design and design change work processes, maintenance practices and maintenance work control, inadequate procedures and procedures revision, corrective action program and learning, and management oversight.

Human error subcategories – those errors identified through INEEL review of Licensee Event Report (LER) and Augmented

1 The phrase "context" as used here refers to combination of the individual and crew characteristics including experience and skill, task requirements, plant systems and conditions, and environmental factors that may influence human error.

Inspection Teams (AITs) data sources. Twenty-one subcategories were identified and definitions for each are presented in Section 3.1.1.

Latent Error –latent errors are those errors that are committed pre-initiator and whose effects are not realized until the event occurs. Reason (1990) notes those latent conditions that influence events can be present for long periods of time before combining with workplace factors including active errors to produce an event.

2. METHODOLOGY

2.1 Approach

For this research, the INEEL reviewed events that had been previously selected by the ASP Program at Oak Ridge National Laboratory (ORNL) and found to have a CCDP of 1.0E-5 or greater. This is consistent with Regulatory Guide 1.174 where the acceptance guidelines for increases in CDF generally do not allow changes greater than 1.0E-5. A subset of these events in which human performance appeared to be an important factor was selected and analyzed. Following the ASP methodology, the INEEL calculated a CCDP using specific standardized plant analysis risk (SPAR) models. The INEEL developed these plant models using the Systems Analysis Programs for Hands-on Integrated Reliability Evaluation (SAPHIRE)[2] PRA software package. To distinguish these models from full PRA models in SAPHIRE, they are called SPAR models.

SPAR models exist for all nuclear power generating stations; however, only limited coverage is provided for operating modes other than full power. Some of the risk significant operating events selected occurred in a plant mode for which SPAR models are not currently available. In those instances, qualitative analyses were performed and human errors that contributed to the event and were present in the LER or AIT sources were noted.

An INEEL team consisting of a plant systems and SPAR analyst, a human factors and HRA analyst, and a plant operations analyst, conducted qualitative analyses of events. The selection process for analysis first emphasized those events for which AIT or incident investigation team (IIT) reports were available. Forty-eight events were identified and reviewed to determine whether human performance contributed to the event. Eleven events had no direct human actions as root causes, and were not given any further consideration. There was no discernible pattern in terms of CCDP for the 37 events with human performance contributions versus those events having limited or no human performance contribution. There was no apparent correlation between the CCDP values and the degree of human performance involvement for the events evaluated. Human performance was an important contributor in all 37 events. All events were analyzed qualitatively, but only 23 events were analyzed quantitatively. In every instance, the team reached consensus regarding the presence of a human failure and the category associated with that failure.

2.2 Event Selection Criteria

Selection of the events for analysis began by review of the LERs and other reports for ASP-identified events that had occurred between January 1, 1992, and December 31, 1997, and that had an ASP-calculated CCDP greater than 1.0E-05. During the course of the study two additional events (Indian Point 2 event on August 31, 1999 and Hatch on January 26, 2000) occurred that were deemed pertinent to the project and were added to the others.

With one exception, these event analyses used Rev. 2QA versions of the Level 1 SPAR models. (e.g., Standardized Plant Analysis Risk Model for Wolf Creek Generating Station 1997). The Rev. 3i SPAR model was used for the Millstone Unit 2 event assessment. Rev. 3i SPAR models, currently under development at the INEEL, incorporate the large loss-of-coolant accident (LLOCA) and medium loss-of-coolant accident (MLOCA) initiating events that are required for the analysis of the Millstone Unit 2 event on January 25, 1995.

SPAR analyses of these events allowed for estimating the contribution of human errors to the increased CCDP. It is not possible to extract this information from the ASP

---

2 K. D. Russell et al., NUREG/CR-6116, Vol. 1-8, Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0, US Nuclear Regulatory Commission, July 1994.

program LER analyses reported in NUREG/CR 4674, Volumes 17 through 25, *Precursors to Potential Severe Core Damage Accident*, because these reports are summaries of earlier analyses. Thus, they typically do not document the base CDP. Calculation of the risk factor increase (RFI) and other event importance measures used in the present study requires the CDP as input. Also, the ASP and SPAR programs have made significant changes to methods and data, and it was decided to employ the latest generation of models.

For each event analyzed with a SPAR model, both a CDP and CCDP were calculated. The SPAR model results do not necessarily match the results reported by the ASP program, nor should they be expected to do so. Differences are due to model version (enhanced detail of components and systems) and analysis methodology differences. For example, the models and software platform for ASP have evolved from split-fraction to linked fault tree analysis. Underlying basic event and initiating event probabilities have been refined as well.

SPAR model analysis was run for each event. Nominal and event-specific sequence CDPs were determined. The contribution of human performance to CDP, RFI, and the event importance were also characterized. Additionally, human performance issues underlying the events were described in detail.

Appendix A contains summaries of events taken from Human Performance Event Database (HPED) and the AIT or LER reports, human error descriptions, indication whether the error was active or latent, and associated error subcategory. Typically, the event assessment for each of the events made use of the analyses performed within the ASP program when those were available.

2.3 Determination of Risk Measures

Risk factor increase and event importance measures were used in the present study. Regulatory Guide 1.174 provides guidance for interpretation of event importance measures.

The contribution of human performance to the event importance was determined in the present study. It was calculated as the ratio of the portion of event importance attributed to human errors, relative to the total event importance. In equation form this is:

Human Event Contribution (%) =

$$\frac{CCDPHE - CDP}{CCDPEvent - CDP} \times 100\%$$

Terms used in the formula:

CCDPHE: the portion of CCDP due to human influences, determined by the analysis team who reached concurrence regarding whether the basic event cause in the LER could be attributed to human performance. Details regarding the screening questions used by the team to support their determination of cause are found in section 3.1.

CCDP: total CCDP for the event

CCDPHE – CDP: event importance due to human error contributions

CCDP Event – CDP: total event importance.

CDP – core damage probability. The likelihood of a nuclear power plant experiencing core damage over a given period of time based on the nominal CDF. This is the base case for comparison to the CCDP in event assessment.

3. EVENT ANALYSIS RESULTS

This section presents CDF, CDP, and corresponding conditional core damage frequency (CCDF) or CCDP results that were used to derive insights regarding the influence of human errors on event risk. Summary data regarding the type of human error present across all events analyzed in this study follows. Human error findings on an event-by-event basis are also presented along with a discussion of error category and subcategory results. For a synopsis of events, refer to Tables A-1 and A-2. Appendix B summarizes each event in terms of the presence of active and latent errors.

3.1 Quantitative Event Analysis: ASP/SPAR and Human Performance Findings

Table 3-1 summarizes the PRA model evaluation findings for events analyzed in this study ranked by event importance. Rev 2QA SPAR models yielded different CCDP values than did the earlier ASP models. These differences reflect model changes made over time. Risk factor increase measures for every event are also presented.

The "ASP reference" column in Table 3-1 includes the CCDP values for individual events that were obtained from the ORNL risk analysis performed in the ASP Program[3].

Event descriptions that appear in this report were developed from LERs and AIT sources reviewed by the INEEL team. LER numbers are supplied for all events reviewed in this report and event dates and LER numbers are obtained from the NRC Sequence Coding and Search System (SCSS) database. Basic event values in the SPAR model were determined as part of the SPAR model development program. A basic event includes the failures of individual components and/or explicitly modeled human actions. In event assessment, the risk associated with the basic event failures present in an operating event are considered and compared to the risk calculated prior to the event. There are different ways in which to characterize resulting differences between the two. For example, the importance of the operating event (CCDP-CDP) or the risk factor increase (CCDP/CDP) can be used to evaluate the difference in risk between the PRA base case and the actual event.

An event importance measure of greater than or equal to 1.0E-6 was used as the criterion for retention of events in this study. This is consistent with guidance suggested by Regulatory Guide 1.174, where any risk increase less than 1.0E-6 is considered insignificant. Additionally risk factor increase was developed as a measure of relative risk significance of an event.[4] This measure is the ratio of the event CCDP to the nominal CDP value.

The human error contribution to the event importance calculated in the present study represents a ratio of the portion of the event importance attributed to human error to the total event importance.

As part of the analysis, the percent human error contribution to event importance was considered. The team reviewed the components failed in the event and asked a number of questions to decide whether the component failure or unavailability was due to or influenced by human error.

[3] NUREG/CR-4674, Precursors to Potential Severe Core Damage Accidents: 1992, A Status Report, Vol. 17-26, Oak Ridge National Laboratory.

[4] The risk factor increase compares the analyzed event CCDP to the baseline CDP (CCDP/CDP). For example, a factor increase of two represents a doubling of the core damage probability when given sets of components are guaranteed/ postulated to be failed. For events with a CDP of 1.0E-05 or greater a factor increase of 1.1 would represent a risk change (delta) of at least 1.0E-06 meeting the guidance of Regulatory Guide 1.174 (1998).

Table 3-1. INEEL Results of SPAR Conditional Core Damage Probability Analyses Ranked by Event Importance.

Analysis No.	ASP Reference and Screening Basis Value (CCDP)	Facility	Event Date	LER and AIT Numbers	Risk Importance Measures: SPAR Analysis CCDP	Risk Factor Increase (CCDP/CDP)	Event Importance (CCDP-CDP)	Human Failure Percent Contribution to Event Importance[5]
1	2.1E-04	Wolf Creek Generating Station 1	01/30/96	482-96-001	5.2E-03	24,857	5.2E-03	100
2	2.1E-04	Oconee 2	10/19/92	270-92-004	3.2E-03	86.5	3.2E-03	100
3	1.2E-04	Perry 1	04/19/93	440-93-011	2.1E-03	242.1	2.1E-03	100
4	2.2E-04	Oconee 2	04/21/97	270-97-001	7.1E-04	2.5	4.3E-04	100
5	1.3E-05	Limerick 1	09/11/95	352-95-008	4.8E-04	9.8	4.3E-04	100
6	2.0E-04	Indian Point 2	08/31/99	AIT 50-246/99-08	3.5E-04	25	3.4E-04	100
7	9.3E-05	McGuire 2	12/27/93	370-93-008	4.6E-03	2.4	2.7E-04	82
8	NA	Hatch	01/26/00	321-00-002	2.5E-04	13.2	2.3E004	100
9	2.1E-04	Robinson 2	07/08/92	261-92-013, 261-92-017, and 261-92-018	2.3E-04	4.2	1.8E-04	100
10	6.5E-05	Haddam Neck	06/24/93	213-93-006 and 213-93-007; AIT 213/93-80	2.0E-04	4.3	1.5E-04	48
11	3.2E-05	Oconee 1, 2, and 3	12/02/92	269-92-018	1.5E-04	125	1.5E-04	100
12	1.8E-05	River Bend 1	09/08/94	458-94-023	1.2E-04	2.5	1.2E-04	100
13	1.8E-04	Sequoyah 1 and 2	12/31/92	327-92-027	1.1E-04	14,103	1.1E-04	100
14	5.5E-05	Beaver Valley 1	10/12/93	334-93-013	6.2E-05	10,690	6.2E-05	100
15	NA 4	Dresden 3	05/15/96	249-96-004	2.6E-05	15.3	2.4E-05	100
16	1.1E-04	St. Lucie 1	10/27/97	335-95-005	3.8E-05	2.9	2.5E-05	100
17	4.6E-05	Seabrook 1	05/21/96	443-96-003	3.E-05	2.3	2.5E-05	100
18	6.5E-05	Comanche Peak 1	06/11/95	445-95-003 and 445-95-004	1.9E-05	146.2	1.9E-05	10
19	6.0E-05	ANO Unit 2	07/19/95	368-95-001	1.4E-05	73.7	1.4E-05	100
20	5.6E-04	ANO Unit 1	05/16/96	313-96-005	9.6E-06	50.5	9.4E-06	100
21	3.7E-05	D. C. Cook 1	09/12/95	315-95-011	3.3E-05	1.2	4.9E-06	80
22	1.3E-04	LaSalle 1	09/14/93	373-93-015	4.5E-05	1.07	3.0E-06	100
23	7.7E-05	Millstone 2	01/25/95	336-95-002	2.6E-05	1.04	1.0E-06	100

[5] Based on analyst assignment of contributions to basic events failed in the risk model. These contributions were then propagated through the PRA risk equation.

The team worked on the events individually and then met to discuss the events and component failures with a set of questions for guidance. The following questions were used:

- Was the likelihood of component failures influenced by inadequate maintenance, surveillance, or testing?
- Did operators or maintenance personnel operate or maintain equipment improperly, influencing the likelihood of failure or unavailability?
- Did work package design, procedure development or reviews influence the likelihood of the failure(s)?
- Did the level of technical knowledge of the staff influence the likelihood of initiating events, failures or unavailability for components modeled in the PRA?
- Did the organization fail to respond to industry notices or delay corrections to known design deficiencies that may have prevented the event from occurring?

The typical methods used to determine contributors to risk or importance to risk require evaluation of the risk equations generated in a PRA. This limits the results to only the risk elements that are explicitly modeled. A considerable amount of additional analysis is needed to get to contributors that are implicitly in the model through data or assumptions. Such an analysis was not within the scope of this study. To gain some insights regarding the involvement of active and latent human errors, an evaluation was made based on the answers to the above questions. Consensus resulting in affirmative answers to any of these questions for a component that was modeled as failed in the PRA resulted in a determination that the percent human error contribution to that component's failure was 100%. This represents a *screening analysis* of the impact of human performance.

The total human error contribution assigned to the event is determined by how the impacted components come together in the logic of the risk equation (i.e., the cutsets coming out of the event analysis). For example, the value of 82% listed for the McGuire 2 loss of offsite power (LOOP) resulting in a reactor trip event represents a calculation of the contribution of human error to a subset of all failed components for that operational event. Since human performance was only responsible for a portion of the failures, the total contribution to the risk increase is less than 100%. The exact contribution is determined after cutsets are quantified. Human performance figured prominently in all events. For instance, the human contribution to the top four events whose importance was on the order of 1.0E-03 or greater was 100%. At the other end of the spectrum, the human performance contribution to events with lower event importance measures was also 100% in most cases. SPAR model analysis for these 23 events resulted in CCDP values that ranged from 9.6E-06 to 5.2E-03. The range for risk factor increase was from 1.04 to over 24,000, indicating a wide range in departures from the base case values, as shown in Table 3-1.

Human errors associated with SPAR-modeled events were combined with those from the qualitatively analyzed events to construct Table 3-2, the Summary Table of Human Error Categories and Subcategories for Analyzed Operating Events (the percentages are based on the total number of errors identified, 270). Table 3-3 presents the percent of events (N=37 events) associated with specific error categories. Table 3-4 provides information regarding the type of accident sequences involved in the events analyzed. Appendix B, Table B-1 presents human error category and subcategory information determined on an event-by-event basis. Appendix C, Table C-1 presents results of a mapping exercise in which the relationship of human errors to the SPAR model basic events for nine events with the highest CDF listed in Section 3.1.1 below.

Human Error Categories

Table 3-2 shows the human error categories and subcategories observed in the events. Categories were derived by their frequency of occurrence as determined through reviews of LER and AIT sources. Supporting definitions for the 21 error subcategories determined by HRA and operations analysts to guide the error analysis are provided in Table 3-2.

Table 3-2. Summary of Human Error Categories and Subcategories for Analyzed Operating Events

Category Description [Count / % of Total Errors (270)]	No. of Latent Errors	No. of Active Errors
Operations (72/27%)		
Command and control including resource allocation	4	14
Inadequate knowledge or training	15	8
Operator Action/Inaction	3	13
Communications	9	6
Design and Design Change Work Practices (70/26%)		
Design deficiencies	24	
Design change testing	9	
Inadequate engineering evaluation and review	18	1
Ineffective abnormal indications	1	2
Configuration management	15	
Maintenance Practices and Maintenance Work Control (58/21%)		
Work package development, QA and use	15	1
Inadequate maintenance and maintenance practices	28	3
Inadequate technical knowledge	5	
Inadequate post-maintenance testing	6	
Procedures and Procedures Development(26/10%)		
Procedures and procedures development	25	1
Corrective Action Program (33/12%)		
Failure to respond to industry and internal notices	8	
Failure to follow industry practices	4	
Failure to identify by trending and use problem reports	9	
Failure to correct known deficiencies	12	
Management and Supervision (11/4%)		
Inadequate supervision	8	1
Inadequate knowledge of systems and plant operations	1	
Organizational structure	1	
Subtotals	220	50
Total = 270/100%		

Table 3-3. Summary of Error Category Presence in Operating Events (N=37) By Percent

Error Category Description	Percentage of Operating Events
Operations	54%
Design and Design Change Work Practices	81%
Maintenance Practices and Maintenance Work Controls	76%
Procedures and Procedures Development	38%
Corrective Action Program	41%
Management and Supervision	30%

Table 3-4. Analyzed Events Classified By Type of Accident Sequences Impacted.

Description	No. of Events	Plant (LER)
Loss or potential loss of emergency core cooling system	8	Catawba 1 & 2 (413-93-002) D.C. Cook (315-95-011) Limerick 1 (352-95-008) Millstone 2 (336-95-002) Perry 1 (440-93-011) Robinson (261-92-013, 261-92-017, and 261-92-018) St. Lucie 1 (335-97-011) Wolf Creek Generating Station (482-96-001)
Partial or complete loss of power (offsite or onsite)	15	Beaver Valley 1 (334-93-013) Byron (454-96-007) Calvert Cliffs 2 (318-94-001) Catawba 2 (414-96-001) Haddam Neck (213-93-006, 213-93-007) Indian Point 2 (247-99-015) LaSalle (373-93-015) McGuire 2 (370-93-008) Oconee All (269-92-018) Oconee 2 (270-92-004) Oyster Creek (219-92-005) Point Beach 1 (266-94-002) Quad Cities (265-93-010) Sequoyah All (327-92-027) Turkey Point (250-92-001)
Reactor coolant system leak, including steam generator tube rupture	2	Ft. Calhoun (285-92-023) Oconee 2 (270-97-001)
Overfeeding of reactor power vessel or steam generator	1	Hatch (321-00-002)
Loss of feedwater or emergency feedwater	7	ANO 1 Unit 1 (313-96-005) ANO1 Unit 2 (368-95-001) Comanche Peak 1 (445-95-003 & 445-95-004) Dresden (249-96-004) Oconee 3 (287-97-003) River Bend (458-94-023) Seabrook (443-96-003)
Loss of annunciators	1	Callaway (483-92-011)
Combination of categories	2	Salem 1 (272-94-007) Loss of Cooling/SI Initiation/PORV initiations South Texas Project (498-93-005 & 498-93-007) Loss of diesel generator (DG) and Emergency Feedwater
Loss of shutdown cooling or loss of reactor pressure vessel level during shutdown cooling	1	Wolf Creek Generating Station (482-94-013)

3.1.1 Human Error Subcategory Definitions

Operations

1. Command & Control Including Resource Allocation - Senior operations personnel lacked adequate real-time command presence and control of activities under the cognizance of the operations department. This includes inappropriate assignment of personnel resources to properly conduct operations and monitor maintenance in progress.

2. Inadequate Knowledge or Training - Operations department personnel lacked adequate system knowledge or practical training for proper conduct of the

activity in progress.

3. Incorrect Operator Action or Inaction - Licensed or non-licensed operators took incorrect actions relative to an activity in progress or failed to take appropriate action when required to mitigate an undesirable result. This includes failure to follow actions contained in established procedures.

4. Communications - Communications between on-watch operations personnel or between operations and other department personnel, such as engineering or maintenance, were lacking or otherwise ineffective.

Design and Design Change Work Practices

5. Design Deficiencies - Either the original design or a change to the existing design was deficient to achieve the intended equipment function.

6. Design Change Testing - Testing performed after a design change was inadequate to properly test the operability of the design change feature.

7. Inadequate Engineering Evaluation or Review - Engineering evaluations or reviews were not performed or if performed, were not adequate to determine sufficiency of the design to achieve its intended purpose. This includes engineering reviews that produced erroneous conclusions.

8. Ineffective Abnormal Condition Indication - The indications available were inadequate or not available to provide effective monitoring for the personnel to take appropriate actions for abnormal conditions.

9. Configuration Management including Equipment Configuration - Either the documentation for equipment configuration was lacking or in error, or the actual equipment was not physically configured as required by valid documentation.

Maintenance Practices and Maintenance Work Control

10. Work Package Development, Quality Assurance (QA) & Use - The work package preparation was deficient in some way, including QA of the work performed. This includes failure to conduct adequate briefings, lack of specificity in the package, or failure to follow the work package to achieve the desired final product.

11. Inadequate Maintenance & Maintenance Practices - The maintenance activity performed was either inadequate, was performed incorrectly, or did not follow skill of the trade expectations. This includes aspects of failure to maintain cleanliness, improper torquing, carelessness, and aspects of preventive maintenance when improperly performed.

12. Inadequate Technical Knowledge (Maintenance) - Maintenance personnel did not possess adequate technical knowledge relative to the specific equipment or system being maintained.

13. Inadequate Post-Maintenance Testing – Post-maintenance testing was inadequate or insufficient to correctly determine the operability of the equipment after the maintenance was considered complete.

Inadequate Procedures/Procedure Development

14. Inadequate Procedures or Procedure Development - Procedures used were not complete, concise, clear, or otherwise in error or in need of revision prior to use. Generally this category refers to operations and surveillance procedures but could apply to generic maintenance procedures as well.

Corrective Action Program and Learning

15. Failure to Respond to Industry & Internal Notices - The licensee failed to properly process, assess, or act upon an industry, NRC or internal company notice that identified an applicable condition that required some action to prevent an undesirable occurrence.

16. Failure to Follow Industry Practices - The licensee failed to follow or learn from a recognized industry practice for maintenance or operation of equipment.

17. Failure to Identify by Trending & Use Problem Reports - The licensee failed to trend an off-normal condition or use existing problem reports to identify an adverse condition that required corrective action.

18. Failure to Correct Known Deficiencies - The licensee failed to correct known deficiencies in a timely manner, which led to undesirable effects in plant equipment or operations.

Management Oversight

19. Inadequate Supervision - Maintenance activities or evolutions in progress did not have adequate supervision to ensure adherence to established requirements.

20. Inadequate Knowledge of Systems & Plant Operations by Management - Management did not have adequate knowledge of plant systems or plant operations to effectively make correct decisions relative to conduct of operations, engineering, or work planning.

21. Organizational Structure - The organizational structure of the licensee impeded efficient and proper conduct of work, engineering or operations activities.

3.1.2 Analysis of Errors Present in Individual Events

Table B-1 Appendix B, presents human error category and subcategory findings for individual events. Tables 3-2, and B-1, collectively address the following two questions: (1) “What were the total number and types of important human errors across events and, (2) “What human error categories and subcategories were present in individual events?”

Reviewing individual events yields potentially unique insights when compared to a broader view across events. Events such as Salem 1 or Indian Point 2 that contain a large number of individual failures would unduly influence the total score in Table 3-2 compared with an events having relatively few failures. In Tables B-1 and B-2, each human error subcategory is presented for each event along with a corresponding error frequency. Thus it is easy to determine the number of events in which a particular human error subcategory was present. The number of human errors does not correlate with risk significance measures. That is, events with the most human errors did not necessarily have the highest conditional core damage probabilities.

A comparison by error category between the total number of human errors (see Table 3-2) and error categories present in individual events (Tables B-1) was performed. Review of the data as a function of either total errors or by percent involvement in events reveals that three categories dominated findings: For example, in terms of total errors, design and design change work practices, operations, and maintenance practices and maintenance work control had the highest occurrence in events. The ordering of these three error categories was different when reviewed as a function of the number of events containing a particular error category. Inspection of Table 3-3 reveals that errors in design and design change work practices contributed to the greatest number of events (81%) followed by maintenance practices and maintenance work controls (76%) and operations (54%).

3.1.3 Human Error Subcategories Findings

Referring to the subcategories presented in Table B-1, page B-5, the largest number of errors were categorized as inadequate maintenance practices (31), followed by design deficiencies (24), and procedures and procedures development (26). Operator knowledge and training contained 23 errors.

In terms of the percent of events affected by a particular error subcategory, a similar trend was noted. Maintenance practices was highest (54%), followed by design deficiencies (49%), and procedures (38%). Maintenance work package errors were involved in slightly more events (35%) than were errors in operator knowledge and training (41%). Errors in communication and errors in configuration management were each present in 27% of events. (page B-5).

There was a trend for events with multiple human error categories such as Indian Point 2 and Oconee Unit 2 1992 to have a large number of individual latent and active human errors present. For example, each of these events spanned 8 or more human error subcategories and each consisted of 20 or more human errors. Other significant events such as Haddam Neck (page B-2) or Sequoyah (page B-4) spanned 6 human error subcategories and had 10 or more individual active or latent human errors.

Linkages among multiple errors are not well described in the HRA literature. Discussion regarding dependency findings is presented in Section 4.

3.1.4 Event Classification

The effects of component failure and/or unavailability were analyzed in one of two ways; by an initiating event assessment or by a condition assessment. An initiating event assessment was performed whenever the event caused an upset in the plant. These events include reactor trips, LOOPs, loss-of-coolant accidents (LOCAs), etc. A condition assessment was performed whenever equipment was failed, degraded or unavailable without a plant response. These types of events typically involve problems with standby components and equipment. Table 3-4 shows the results of these analyses.

From Table 3-4, it can be determined that 41% of events involved partial or complete loss of onsite or offsite power. The next most frequent effects were loss of emergency core cooling system (ECCS) (22%) and loss of feed water (19%).

The diversity of the human errors, plant designs, and nature and number of failed and unavailable components within each category precluded identification of common themes or trends in events. From this it may be concluded that human errors are probably most usefully viewed at a higher level such as in Table 3-2 in this section.

The team also compared the human performance evident in the five events with the highest CCDP to events with the lowest CCDP. No differences were identified between causes of the events or responses to the events. The length of the event, the required response to the event, and the number and type of component failures and human errors followed no discrete identifiable pattern. Similar conditions appeared in both the highest five and lowest five events (by CCDP). For example, Hatch Unit 1 and Oconee 1, 2, and 3 1992, which had higher CCDPs, involved design process inadequacies. Similarly, Arkansas Nuclear One (ANO) 1 Unit 2 1996, with a lower CCDP, involved design process and design review inadequacies. The Perry and 1996 Wolf Creek Generating Station events, with high CCDPs, exhibited inadequate maintenance practices and management controls. Similarly, the LaSalle 1993 and ANO Unit 1 1996 events, with lower CCDPs, also exhibited inadequate maintenance practices and timeliness of corrective actions program. There were slightly more active human errors in the high CCDP group but this was mainly attributed to by the 1996 Wolf Creek Generating Station event.

4. EVENT ANALYSIS DISCUSSION

The analyses performed to date underscore the significant contributions that human performance has made to operating events. This includes human errors that caused event initiation, equipment unavailability, or demand failures. Models were used to analyze the sensitivity of plant risk to these human errors. In addition to human errors, random system and equipment failures also occurred during several events.

4.1 Event Importance and Risk

Event importance measures for the 23 events ranged from 5.2E-3 to 1.0E-6. The percent contribution of human error to event importance ranged from 10% (Comanche Peak 1) to 100% for the next19 events analyzed. Three other events demonstrated strong human error contribution to event importance (i.e., McGuire 2, 82%; Haddam Neck, 48%; and D.C. Cook, 80%).

The risk increases shown in Table 3-1 were due to errors committed by personnel and organizations that operate and maintain these plants. For example, component failures due to human error led to initiating events at Oconee Unit 2 1992 and Dresden 3. The corresponding event importance for the Oconee 2 event was 3.6E-03, the event importance for Dresden 3 was 2.6E-05.

Human errors resulted in initiating events without additional component failures. Such events occurred at Sequoyah 1 and 2 1992 (CCDP = 1.1E-04) and Beaver Valley 1 1993 (CCDP = 6.2E-05). These events have CCDPs that represent a noteworthy departure from the nominal case.

During the course of the analysis, 16 initiating event (IE) assessments were conducted, including LOOP, steam generator tube rupture (SGTR), small loss-of-coolant accident (SLOCA), and transient (TRANS). Two of the events (McGuire 2 and ANO Unit 1) combined two initiating event assessments.

The initiating event for the Sequoyah Unit 1 operating event involved a circuit breaker failure that led to a LOOP and was the result of a failure to test the devise prior to installation and in proper planning of the maintenance.. The initiating event at Beaver Valley involved maintenance crew errors during an outage leading to inadvertent application of 125 V DC in the switchyard. This resulted in the opening of seven breakers in the 345 kV system; three breakers in the 138 kV system, initiating the loss of electrical load at Unit 1. At Dresden 3, the failure of a feedwater regulating valve (FRV) leading to subsequent reactor trip and ECCS actuation could be traced to maintenance practices and running with only one FRV operational. At Oconee 2 1992, switchyard faults resulting from failure to respond to industry notices and internal engineering notices led to a LOOP, the recovery of which was complicated by inadequate procedures and poor work package preparation. During other operating events analyzed, human errors resulted in other equipment unavailability. As a result of these unavailabilites, plant systems did not perform their intended functions when demanded to do so by an automatic signal or manual command.

At Seabrook Unit 1 1996, nonstandard maintenance practices for seal installation, and lack of integrating information regarding previous seal failures, coupled with lack of specific direction to use dial indicators as required during maintenance, led to sparking in the turbine-driven emergency feedwater system (EFW) pump during a surveillance test. Lack of design test adequacy resulted in main steam safety valve failure to close at ANO, Unit 1, and main feed pump failure to run. Latent failures in the design review process for ANO, Unit 2 contributed to auxiliary feedwater (AFW) motor-operated valve common cause failure. Design deficiencies, combined with configuration management problems at Indian Point 2, resulted in loss of vital AC power and loss of DC power. Key to this event was failure to control setpoints on safety-related equipment and failure to maintain the load tap changer in position as required by the plant's licensing basis.

At ANO Unit 1 , operations continued with multiple workarounds that challenged operator response to the transient. There were longstanding deficiencies with the safety parameter display system that forced operators to perform hand calculations. Steam generator design deficiencies complicated condenser response during the event, and known problems with the atmospheric dump valves caused concern regarding potential for thermal binding of the valves.

4.2 Latent Errors

Latent errors at the 1996 Wolf Creek Generating Station event included errors in warming line design, lack of technical knowledge regarding conditions that cause frazil icing, failure to respond to industry notices, errors in technical specification interpretation, and maintenance failures for packing of the turbine-driven auxiliary feed pump. These factors, coupled with active errors of declaring equipment operable without performing either engineering evaluation or root cause analysis and failure to transfer information concerning the state of the ultimate heat sink, contributed to the event. The risk factor increase for this event, 24,578, was the largest observed in the sample of operating events analyzed. It is significant that almost all of this increase in risk was due to human performance issues. The event importance for this event was 5.2E-03. Human performance was a key factor in the initiation of these events and the risk increase that resulted.

Qualitative analyses of all events produced further insights regarding the role of human performance in operating events. Table 3-2 summarizes human error categories[6] and subcategories.

The errors that contributed most often to plant events and caused the greatest increases in plant risk were latent errors. Two-hundred and seventy errors were identified. Of these, 19% were active and 81% were latent. This situation reflects the fact that most often active errors have immediate observable impact. Latent errors can accumulate over time until they are manifest by the right conditions.

Review of these data suggests that latent errors, including those associated with maintenance, were important contributors to the significance of the highest conditional core damage probability events that have occurred in recent years. However, latent errors are seldom explicitly modeled in PRAs, instead they are combined into a single equipment failure event. Data on latent errors would provide a more specific description or a root cause for this equipment failure event.

Functional failures and component failures can be introduced by a variety of human and organizational sources, some of which influence the significance of operating events. In general, the work processes by which human errors are introduced include design review, configuration management of drawings, procedures, and equipment; maintenance, surveillance, and corrective actions. In a later work based on the review of numerous major accidents from around the world, Reason (1997) introduced the term *latent conditions*. This was to characterize problems resulting from poor design, gaps in supervision, undetected manufacturing defects, maintenance failures, unworkable procedures, clumsy automation, shortfalls in training, or less than adequate tools and equipment. Such conditions may be present for many years before they combine with local circumstances and active failures to cause operating events.

4.3 Multiple Errors

Multiple errors and failures occurred in the events analyzed. On the average these events contained four or more errors in conjunction with hardware failures. Fifty percent of events contained five or more errors. Many events contained between six and eight errors. Individual errors were mostly minor, insufficient by themselves to cause an event. Their effects are cumulative and challenged plant systems and resources. For example, an

[6] Attempts were made to assign a single error to an individual performance category. In instances where an error crossed two categories, a 0.5 value was assigned to both error categories. This prevented double counting of a single error. In this present study, there are six instances where representation for an error in more than one category is appropriate.

inadequate design review may be insufficient to produce a major event. However, it can result in a latent condition that leads to failure once certain conditions occur. For example, in the 1996 Wolf Creek Generating Station event, the warming line design was inadequate. However, this error did not become apparent until frazil-icing conditions were present.

4.4 Dependence

Dependence within events can be inferred in a number of different ways. First, there is dependence among human errors such as multiple latent failures involving maintenance practices or engineering practices. For example, at Wolf Creek (1996) engineers failed to rigorously test and verify assumptions regarding frazil icing documented in the plant's specifications that were used by the operations personnel. This influenced the failure of the crew to detect and recognize frazil icing conditions. Thus, latent errors combined to influence the probability of an active error, the ability of the crew to detect and recognize the frazil icing conditions.

In some instances, through common cause mechanisms, human errors can impact more than one basic event. At South Texas Project, errors committed while performing a common task caused both diesel generators to become unavailable.

Additionally, errors can influence the likelihood of failure for one component that can, in turn, influence the likelihood of failure for subsequent components in a particular event sequence. At Wolf Creek Generating Station, human error contributed to traveling screen freezing. Failure of the traveling screens in turn, failed multiple systems due to loss of ultimate heat sink.

In the present study, INEEL performed a preliminary mapping analysis on a sample of events[7] to: (1) identify evidence of multiple errors combining to cause or contribute to a single basic event, (2) evidence of a single error causing or contributing to a single basic event, and (3) evidence of multiple errors combining to cause or contribute to multiple basic events. This analysis is summarized in Table 4-1. The following summarizes general findings about the type of dependency identified through analysis of events.

4.5 Relation of Errors to PRA Basic Events

<u>Multiple Errors Mapping to A Single PRA Basic Event.</u> For example, the LOOP initiating event at Indian Point 2 is an example of multiple human errors (6) causing or contributing to the initiating event. The diesel generator basic event in that model (EDG #23) also contains evidence of multiple errors (3) causing or contributing to one basic event. Three human errors combined to cause or contribute to common cause failure of the suppression pool strainers at Limerick 1.

<u>A Single Error Mapping to a Single PRA Basic Event.</u> Limerick 1 provides evidence of a single human error causing or contributing to a transient initiating event, i.e., engineering review of test results on the safety relief valve (SRV) failed to recognize seat leakage coming from the pilot valve. An improper valve lineup at Haddam Neck caused or contributed to an increased failure rate for the Power Operated Relief Valve (PORV).

<u>Multiple Errors Mapping to Multiple PRA Basic Events.</u> At Robinson 2 two human errors caused or contributed to three basic events in the PRA model. Errors in debris removal and inadequate QA of system cleanliness caused or contributed to the failure of two safety injection trains. The 3rd train was modeled as having increased potential for failure due to this common cause failure mechanism.

In the Wolf Creek Generating Station, Perry, and Robinson events, human error caused or contributed to widespread safety system impacts throughout the plant. The Wolf Creek event was a failure of the ultimate heat sink, the Perry event was a failure of all ECCS systems, and the Robinson event was a failure of all safety injection.

In other cases, human error caused or contributed to hardware failures that triggered

[7] Ten events from Table 3-1 having the highest CCDP were selected for analysis and are presented in detail in Table C-1.

the initiating events, and which also degraded response to the events. This includes the Oconee 1997 SLOCA with failure of 1 train of high pressure injection (HPI) cold leg injection, and the Limerick transient and loss of ECCS.

Differences were noted regarding the mapping of human error to PRA basic events versus operating events. In the case of PRA basic events, multiple errors were most frequently observed to cause or contribute to single basic events. In the case of operational events, multiple errors were observed most frequently to contribute to or cause multiple system or component failures. In important events human error's impact is widespread causing

Table 4-1. Summary of Human Error Contribution to PRA Basic Events Included in SPAR Models

Event	Human Error Mapping to PRA Basic Event Failures	Affected Basic Events	Involved Components or Systems
Wolf Creek (1996) – Frazil icing buildup leads to potential loss of ultimate heat sink	7 Human errors combined to cause or contribute to 1 TRANSIENT initiating event and 12 Basic Event failures	1 Transient initiating event These 12 basic event failures included the common cause failure of : Auxiliary feedwater (AFW) pumps, Chemical volume and control (CVC) pumps, High pressure injection (HPI)pumps, Residual heat removal (RHR) pumps, and Emergency diesel generators (EDGs). And loss of individual component function for: AFW pump, CVC pump, HPI pump, RHR pump, RHR heat exchanger, and EDG. Other basic events included Main feedwater human error – No recovery	A-train for auxiliary feedwater (AFW),centrifugal charging pump (CCP), diesel generator (DG), high pressure injection (HPI) pump, and the residual heat removal system (RHR)
	1 Basic event did not involve human error	Failure of the C train turbine driven AFW	
Oconee 2 (1992) – Manipulation of battery charger and bus transfer problems leads to LOOP	3 Human errors combined to cause or contribute to a LOOP initiating event	1 LOOP initiating event	
	10 Human errors combined to cause or contribute to 1 basic event failure	Common cause failure of both Keowee Units	Keowee hydro units
	2 Human errors combined to cause or contribute to 2 basic event failures	Failure of main feeder buses 1 &2	Keowee hydro units and main feeder buses 1 & 2.
Perry (1993) – Failure of all suppression pool strainers leads to failure of all emergency core cooling	4 Human errors combined to cause or contribute to 1 Basic event failure	Common cause failure of suppression pool strainers	RHR suppression pool strainer

Oconee 2 (1997) – Small LOCA condition assessment with assumed failure of HPI cold leg injection path	6 Human errors combined to cause or contribute to a SLOCA initiating event and 1 basic event failure	1 Small LOCA initiating event Failure of HPI cold leg injection path A	HPI injection cold leg path A
Limerick 1 (1995) - Poor testing of safety relief valves; material control and cleanliness problems lead to common cause failure of suppression pool strainers.	1 Human error caused or contributed to the TRANSIENT initiating event and one basic event failure 3 Human errors combined to cause or contribute to 1 basic event failure	1 transient initiating event Main steam safety relief valve Common cause failure of the suppression pool strainers	Main steam safety relief valve (MSSRV) Suppression pool strainers
Indian Point 2 (1999) – Reactor trip followed by spurious trips leads to LOOP	6 Human errors combined to cause or contribute to a LOOP initiating event 3 Human errors combined to cause or contribute to 1 basic event failure 3 Human errors combined to complicate event response but did not directly cause or contribute to any basic event failure	1 LOOP initiating event Failure of emergency diesel generator 23	Station auxiliary load tap changer Emergency diesel generator (EDG 23)
Hatch (2000) – Partial loss of feedwater event	1 Human error caused or contributed to a TRANSIENT initiating event 3 Human errors combined to cause or contribute to 1 basic event failure and many failed sequence recoveries	1 transient initiating event Operator failure to control HPI sources Transient sequence XX recovery sources	Inlet valves HPI sources
McGuire 2 (1993) – Failure of turbine generator runback feature leading to LOOP	3 Human errors combined to cause or contribute to a LOOP 4 Human errors combined to cause or contribute to a SGTR initiating event and one basic event No human errors mapped to 5 basic events involving PORVs	1 LOOP initiating event 1 steam generator tube rupture initiating event Failure to isolate a ruptured steam generator Unaffected basic events: PPR –SRV – CO PPR-SRV-CO-SBO,PPR-MOV FC, CC, PPR- SRV – CC- PRV1	Turbine generator runback & bus line insulators Steam generator (SG)
Robinson 2 (1992) – Maintenance and design leading to start-up transformer trip followed by LOOP	2 Human errors combined to cause or contribute to a LOOP initiating event 2 Human errors combined to cause or contribute to 3 basic events	1 LOOP initiating event Common cause failure of safety injection pump trains A,B, & C	Start up transformer Safety injection (SI) pumps
Haddam Neck (1993) – Motor control center bus failure and PORV failure	2 Human errors combined to cause or contribute to 1 basic event 1 Human error caused or contributed to 1 basic event	Failure of motor control center (MCC) #5 Failure of Power operated relief valve (PORV)	Electrical bus failure PORV

support system failures, safety system failures, or a combination of initiating events and responses to those events. In some cases, similar errors and failures were involved. For example, two of the three boiling water reactors (BWRs) reviewed in Table C-1 experienced common cause failure of the suppression pool strainers as a result of multiple human errors.

4.6 Inattention to Recurrent Problems

Utility inattention to recurrent problems was evident in 41% of events. This included inattention to NRC inspection findings, internal engineering department notices, industry notices, vendor notices, and previous LERs. In many cases, problems that should have been known from previous experience were not identified, or acted upon. This includes operating with known design deficiencies, permitting "workarounds" (i.e., alternate operator actions – usually manual actions to operate the system), or documenting problems and solutions but failing to take action in time to prevent an equipment or system failure. Failure to follow plant or industry trends, respond to industry notices, owners' groups reports, or pay attention to recurrent problems figured prominently.

4.7 Active Errors

Of the total active, post-initiator errors, 28% involved command and control and resource allocation failures. For example, command and control between Oconee Unit 2 1992 and Keowee hydroelectric station compromised plant response. Keowee staff was performing actions that affected emergency power at Oconee without notifying or obtaining permission from Oconee control room management. The Beaver Valley 1 LOOP event failed to include operations in maintenance planning and there were no clear-cut protocols for the Unit 2 staff to direct operations at the switchyard. At McGuire 2, during the LOOP event the duties and responsibilities for the senior reactor operator (SRO) during emergency conditions were not well defined. Command and control was an issue at other plants. Staffing problems and interference from the field also influenced crew response at Salem 1 when cooling water was lost during river grass intrusion.

Based on the experience of the authors, these types of command and control failures do not appear to be explicitly modeled in PRAs. As with most details of pre-initiator errors, these types of problems are included in the raw data used to determine the component failure rates or test and maintenance unavailabilities.

4.8 Inclusion of Errors in PRA

Many of the significant contributing human performance factors observed in operating events are not explicitly modeled in the human reliability analyses of the current generation of PRAs, including the individual plant examinations (IPEs) (see Section 5 and Appendix D for more discussion). The current generation of PRAs does not explicitly treat differences among types of latent errors, or the combining of multiple latent errors determined by analysis to be important in these operating events.

Most HRAs in current generation PRAs separate human actions into two basic categories: pre-initiator actions and post-initiator actions. Pre-initiator actions are those that, if performed incorrectly, can impact the availability of systems and components when they are needed to respond to an accident initiator. These actions typically include errors in calibrating instrumentation or errors in restoring systems after maintenance. Post-initiator human actions are typically classified as either response actions (actions required for proper plant response, generally called out in procedures) or recovery actions (restoring failed or unavailable systems in time to prevent undesired consequences).

By their very nature, latent human errors tend to be more closely aligned with pre-initiator human actions and failures of standby components and systems upon demand. NUREG-1560 found that while all of the various PRAs addressed pre-initiator human actions, their treatment varied across plants. Several PRAs addressed pre-initiator human actions by arguing that their failure probabilities are insignificant or contained within the system unavailability data. Other PRAs used a screening approach and only quantified explicitly those events that proved important after initial accident sequence quantification. None of the IPEs performed an analysis that explicitly factored observed latent errors into the model or assign human action failure probabilities based upon multiple, underlying, latent conditions.

The review contained in NUREG-1560 determined human performance to be an important contributor to risk. For example, in the pressurized water reactor (PWR) PRAs, switchover to sump recirculation was observed to account for 1 to 16% of CDF (average of 6%). Contribution to CDF for feed and bleed initiation was observed to range from 1-10% with an average of 4%. An overall impact of the set of all modeled human actions was not provided as part of the report, but in some instances a single human action was involved in as much as 40% of the CDF. Generally, PRAs find that human performance is important in sequences that require operator actions to initiate or operate plant systems to mitigate the effects of an initiating event and subsequent equipment failures. Examples of such actions include switchover to sump recirculation mode, initiation of "feed and bleed" or once through core cooling, and depressurization and cooldown.

In the events studied, both BWRs and PWRs were susceptible to the influence of latent errors. For example, known design problems for components and systems that have not been acted upon by the licensee are considered to be latent errors. Inadequate engineering evaluations, problems in configuration management, and poor work package preparation, are additional examples of latent errors. The distribution of significant events in this study follows the general percentages among BWRs and PWRs in the U.S.

Of the 48 events initially selected for this study, 11 were determined to have no human error contribution, 23 were quantitatively evaluated and 14 were only qualitatively evaluated. For the events where a numerical contribution was determined, the average human error contribution to the change in risk was 62%. Recall that the events were selected because they were thoroughly documented, the effects of human performance were well characterized, and the influence of human performance was likely to be noteworthy. This selection of events naturally skews the results to emphasize human performance significance.

Not withstanding, it can be stated that improper human performance can severely impact risk and changes in risk.

In contrast to errors modeled in most PRAs, omissions and commissions in following procedures or taking actions within a given time were not found to be the major determinants of risk increase. Furthermore, active human errors, although important, represented a smaller proportion of human errors and failure events. Latent errors were the primary contributors to the events studied; active failures by operations personnel were not. Of course, the events modeled in the ASP program are only precursors to core damage and rarely proceed far enough to challenge many of the procedures or actions modeled in a PRA.

In most cases, it was not possible to say that a single error or failure caused the event, but that multiple factors were contributors. Combined with other failures, however, human errors produced challenges to plant systems and resources. In many events, inadequate attention to industry and NRC notices, as well as known deficiencies in the plant, contributed to the event. In nearly all cases, plant risk more than doubled as a result of the operating event and in some cases increased by several orders of magnitude over the baseline risk presented in the PRA. This increase was due, in large part, to human error.

Even though the events selected were biased to emphasize human performance issues, the large number of latent errors and conditions identified in these operating events suggests a degree of detail not previously modeled. This level of detail may be needed if individual contributions to hardware failures are desired (for example, in studies where mechanisms by which the prevention or detection of latent errors could be improved). In addition, further analyses may be needed to better understand the impact of smaller, less-significant errors, and the mechanisms by which they combine to produce larger, more significant effects. Dependencies among latent and active human errors should be investigated to determine impacts on failure probabilities.

Other issues that may warrant additional study include the work processes and practices by which licensees control maintenance work, and mechanisms by which recurrent problems and notices are addressed. Note that the recent implementation of the NRC's maintenance rule and industry corrective action initiatives may have improved detection and correction of latent errors; however, no summary evidence is available at the current time to confirm this.

In terms of modeling, there is a question of how best to integrate the potential impact of latent errors on accident sequences in PRAs. For example, is the true impact of human error adequately assessed in PRA when latent errors are only accounted for in equipment failure? Should new contributors to initiators or sequences be considered? Should changes to screening approaches be considered to better account for latent error? Are there enough similarities in the number and types of latent errors evidenced in events that failure rates and distributions for them can be determined?

Are the existing logic structures used in PRA the appropriate ones for incorporating this information? How does this information from events complement or support current efforts in the field of HRA to address the issues of errors of commission and context? What further research of events is needed to support the technical basis underlying the NRC inspections process?

The NRC has issued its recommendations for reactor oversight process improvements and implementation (SECY-99-007). Based in part on insights from the review of operating events obtained from this project, a need was identified to characterize the extent to which performance issues observed in significant operating events will be accounted for in the reactor risk oversight process.

5. SUMMARY, FINDINGS, AND IMPLICATIONS OF ANALYSIS

A sample of 48 events identified as significant through the ASP program was selected and analyzed to determine the impact of human performance on risk contributors. In all but 11 cases, the influence of human performance was present. Those 11 events were not analyzed further. The 37 remaining events were evaluated qualitatively. Where possible, events were also analyzed using SPAR PRA models. Analysis results suggest a number of findings regarding the influence of human performance on this sample of significant operating events.

5.1 Analysis Findings

5.1.1 Effect of Human Performance

Human error contributed significantly to risk in nearly all events analyzed. Forty-one percent of events involved partial or complete loss of either onsite or offsite power, twenty-two percent involved loss of ECCS, and nineteen percent involved loss of feedwater. In the events, the event importance's ranged from 1.0E-6 to 5.2E-3. A characterization of the contributions to the risk increases shows that human performance contributed between 10% and 100% for any given operational event. The average human error contribution to the change in risk was 62%.

5.1.2 Latent Errors

Latent errors were present in every event analyzed and were more predominant than active errors by a ratio of 4 to 1. This is similar to other recent studies concerning the impact of organizational factors (Reason 1998) and the diffuse impacts of work processes upon plant risk (Gertman et al., 1998).

Latent errors were noted in all facets of performance studied, including operations, design and design change work practices, maintenance practices and maintenance work controls, procedures and procedures development, corrective action program and management and supervision. The degree of latent error involvement in risk-significant operating events warrants attention. A study of the contribution of latent errors to the important basic events in models of plant risk would provide useful information especially in cases where the cause of the failure is important. This would help to focus resources on plant programs that are important contributors to plant risk.

A related need is further analysis of the impact of smaller, less significant errors. Specifically, this research raises the questions of how they combine to produce larger, more significant effects, and what the risk implications are associated with dependencies among multiple human errors.

Errors and deficiencies in work practices can be a root cause for latent failures. Implicitly, work process deficiencies were present in a large number of events analyzed and are evidenced by errors in design and design change practices, maintenance practices, maintenance work controls, and corrective action program failures.

5.1.3 Multiple Human Errors

Without exception, operating events analyzed in this study included multiple human error contributing factors. On the average, the 37 qualitatively analyzed events contained 4 or more human errors in combination with hardware failures. Fifty percent of events contained five or more human errors. Many events contained between six and eight latent human errors. These errors were diverse, and included factors such as failure to enforce standards, lack of quality assurance during procedure writing, duties and responsibilities not clearly understood during events, failure to trend and address previous problems, and failure to test after equipment malfunctions.

5.1.4 Human Errors Impact PRA-Significant Equipment

Human errors can result in the failure or increased likelihood of failure of PRA-significant equipment. Of the 37 events involving human performance issues, 23 were analyzed by quantitative methods. The risk increases associated with these events ranged from 1E-6 to 5.2E-3. In the vast majority of these events, human errors were prevalent. They were sometimes modeled explicitly in the PRA model, but for the most part, the impact was reflected in component failure or increased unavailability of hardware components modeled in the PRA. Findings highlight the need for increased understanding of the risk impact of latent errors on operating events as a key step in furthering our knowledge regarding risk contributors. This trend regarding the importance of latent conditions and errors may change as the sample of events is increased, but based on the present study, this finding is unequivocal.

Human error was determined to contribute to component failures. There were three events where a single human error contributed to a single PRA basic event, and seven events where multiple human errors contributed to multiple PRA basic events. Dependency between maintenance and design errors, and dependency between preceding and subsequent component failures in several event sequences suggest that the issue of the representation and failure rates of dependency in HRA needs to be given greater consideration.

Failure rate information that reflects combining human errors in events is also needed. To do so first requires being able to characterize the linkages between these errors and functional, system, and component failures. Since many errors resulting in equipment unavailability and demand failure occurred as a function of inadequate work processes, research aimed at understanding work process influence on maintenance and operations may be key to understanding these errors and associated dependencies. A better understanding of latent errors would also lead to the development of HRA methods that are more robust in modeling human error inter-dependencies and the contribution of pre-initiator human errors.

5.1.5 Error Category Findings

Design and design change work process errors were present in 81% of events, maintenance practices and maintenance work control errors were present in 76% of events, and operations errors were present in 54% of events. The percentages of all other error categories ranged from 30-41%. Additionally, more maintenance and operations errors mapped to basic events in the PRA model than did design and design change errors.

Errors in procedures and procedure development were present in 38% of events, management and supervision errors were identified in 30% of events. The analysis team expected the presence of errors in these categories above. The extent of recurrent plant problems and errors in the corrective action program was less expected and is treated separately below.

5.1.6 Recurrent Problems

Forty-one percent of events demonstrated evidence of failures to monitor, observe, or otherwise respond to negative trends, industry notices, or design problems. This suggests that inadequacies in licensee corrective action programs may play an important role in influencing operating events. Indicators for determining when these processes are flawed, and what impacts on safety and performance may be expected, would prove useful.

5.2 Areas Identified for HRA Enhancement

This research has identified several areas for potential enhancements to HRA models, data, or quantification. The six potential enhancements identified by the analysis team for future consideration are listed below.

1) A method for using human performance data from operating events to support HRA should be considered. Updates to human error probability (HEP) reference values and distributions based upon operating experience would be a significant improvement for HRA. This study

demonstrates an approach for identifying those errors leading to unsafe acts by mapping multiple latent errors to PRA basic events.

2) HRA applications can be directed toward characterizing latent errors and a portion of work process variables present in operating events. Guidelines on how this can be integrated with existing fault tree and event tree models, including level of HRA analysis, should be developed as part of the HRA process.

3) Data on activities related to maintenance, surveillance, test, calibration, installation, and corrective action prioritization and processing could provide a basis for assessing the root causes of equipment failures rates and for potential recovery actions and decisions with risk impact potential.

4) The mechanisms by which small, multiple errors impact risk and the linkages by which they combine should be better understood. After an initial human error, dependency calculation methods often increase subsequent human error probability (HEP) estimates. However, many small errors are often not considered or are discarded after the screening analysis. Often these small, multiple errors cut across different systems and quite different components, do not become important until the occurrence of the initiating event.

5) It is difficult in many situations to consider the impact of variables such as latent error that are only considered implicitly. The percentage of hardware unavailability due to human error as opposed to random hardware failures is not known. If this were determined, then the risk reduction associated with human reliability in these areas could be better approximated.

5.3 Relation of Event Duration and Event Severity

The events were analyzed for duration to see if the events with a higher conditional core damage probability occurred over a longer period of time than others. The top four events (i.e., those having the highest CCDPs) were compared to those with the lowest CCDP numbers. We questioned whether events that were mitigated more slowly might pose a greater risk than those that were handled more quickly. No such trend was found.

5.4 Errors in Operations

For events involving errors related to operations, two types dominated. In the first type, operators erred due to deficiencies in command and control and resource allocation (Salem, Wolf Creek Generating Station, Oconee–Keowee, McGuire). The second major source of problems during operations was ineffective diagnosis (Catawba, Oconee Unit 3). Additionally, compromised situation awareness and communications errors further influenced events. Insufficient technical understanding coupled with inadequate procedural guidance also degraded operator performance. Currently, HRA methods do not typically address problems in communications other than through performance shaping factors.

The most often-observed human error category for active errors was command and control and resource allocation. The dynamics of these factors in operating events are not well understood. There are no HEPs in traditional sources either for command and control errors, or for aspects of distributed decision making such as those errors that occurred in the Oconee–Keowee and the Salem river grass intrusion events. A Technique for Human Event Analysis (ATHEANA) and other methods may provide a structured means to characterize important factors used in deriving estimates via consensus expert opinion. However, there is no data set of peer-reviewed values or distributions to which one can turn for guidance when performing quantification.

5.5 Relationship to IPE and Current Industry Efforts

5.5.1 Relationship of Errors in Events to IPE

Most of the latent human errors observed in the 37 qualitatively-analyzed operating events are neither explicitly modeled nor documented in the current generation of utility IPEs. Such errors are generally captured in the unavailability values assigned to the impacted equipment or components (and their failure modes). In this manner the overall numerical risk calculations are more nearly complete with respect to latent human errors than the explicit description of these errors in the PRA. The IPEs (see NUREG-1560) primarily estimate the human contribution to plant risk through explicitly modeled operator actions in response to upset plant conditions. While this is a legitimate human performance source of risk, this study shows that it is not the only source. By not explicitly modeling the latent human errors, sensitivity and importance studies to determine the influence of human performance on risk using the IPEs may under-estimate the impact of human performance on risk.

5.5.2 Ties to Industry Efforts

The Institute of Nuclear Power Operations (INPO) documents several practical suggestions for promoting excellent human performance at nuclear power plants (*Building on the Principles for Enhancing Professionalism: Excellence in Human Performance,* Institute of Nuclear Power Operations, September, 1997). They emphasize that these suggestions should be followed during design, construction, operation, and maintenance rather than just targeting work outcomes (an end-state). "Human error," they state, "is caused by a variety of conditions related to organizational practices and values." Therefore, "to optimize task execution at the job site, it is important to align organizational processes and values." Effective team skills are an important part of this. But at the same time, INPO emphasizes that individuals need to conscientiously confirm the integrity of defenses. Individuals can do so by using procedures rather than shortcuts, and when plant conditions are different than those assumed by procedures, individuals need to consider their own knowledge. Excellent workers correct procedure deficiencies before proceeding on a job. When unanticipated or unfamiliar conditions are discovered, high-performing individuals stop work and involve the work team, collaborating and using collective knowledge and experience to determine the most effective course of action. High-performance leaders actively consult others to identify potential failure-likely situations or flawed defenses. Managers are encouraged to simplify work processes so that they are easy to use. Managers are encouraged to reduce or eliminate ineffective coordination among work groups, unrealistic time demands, and inaccurate procedures.

INPO stresses that whenever a special test or an infrequent plant evolution is planned, managers should consider the following:

> "…establish clear lines of authority, consider the adequacy of technical procedures and guidance, effectively communicate between groups so as to preclude delays, specify the oversight during the evolution, plan contingencies for off-normal and unexpected plant conditions, and make sure there is access to necessary technical support." (INPO 1997)

Their suggestions are supported by this study of operating events. However, modeling and evaluating these factors is not within the scope of most HRA/PRA efforts and factors such as contingency planning, oversight, and communication among groups are often uncharacterized. Note that the chemical industry (in Murphy 1997) suggests identifying increases in the number of work orders, changes, and failures in order to gauge the safety and risk of a facility. This may prove to be an area worth further consideration for the nuclear industry. Identifying inadequacies in work orders can help to uncover flawed work processes and inadequate maintenance practices that can result in hardware unavailabilities. Assessing the adequacy of processes supporting procedure design and review is potentially valuable in understanding and characterizing work process contribution to risk significant demand failures and component unavailability.

Present findings point to the risk importance of latent errors, maintenance practices, corrective action programs, procedure adequacy, use of resources, implementation of industry findings, etc., in operating events.

These findings are supported elsewhere.
In a review of 342 events by participating countries from July 1996 through June 1999, the Organization for Economic Cooperation and Development (OECD) (2000) notes as an important topic for increased study, the experience of human errors in combination with system failures. It notes that sufficient resources should be allocated for study and compilation of data to further fundamental understanding. This

research confirms this conclusion.

The OECD report also notes that problems such as those found in work planning and processes, quality control of documentation, and maintenance errors were involved in incidents at nuclear power plants. The findings are consistent with the present study. On the basis of reports gathered from various national reporting systems, the OECD reports a significant number of latent failures in safety systems associated with incidents. These failures involved a broad class of systems and a great variety of failures. Although they do not speak directly to the issue of small multiple failures in events, the OECD data support the findings from this study.

6. REFERENCES

1. Belles, R.J., et al. *Precursors to Potential Severe Core Damage Accidents: 1997,* NUREG/CR-4674, ORNL/NOAC-232, Vols. 14 -28, November 1998.
2. Gertman, D. I., Hallbert, B. P., Schurman, D. L., and Thompson, C. Management and Organizational Factors Research: The Socio-organizational contribution to risk assessment and the technical evaluation of Systems (SOCRATES), in *Proceedings of 4th International Conference on Probabilistic Safety Assessment and Management* PSAM-4, A. Mosleh and R. A. Bari, Eds., New York: Springer-Verlag, September 13-19, 1998.
3. Gertman, D. I., Blackman, H.S., Haney, L.N., Seidler, K.S., and Hahn, H.A. INTENT: A Method for Estimating Human Error Probabilities for Decision Based Errors. *Reliability Engineering & System Safety* 35, 127-136, 1992.
4. Hall, R. E., Fragola, J., and Wreathall, J. *Post Event Human Decision Errors: Operator Action Tree (OAT)/Time Reliability Correlation*. NUREG/CR-3010, Washington, DC (USA), 1982.
5. Hannaman, G. W., Spurgin, A.J., Lukic, Y. *Human Cognitive Reliability Model for PRA An*alysis. Draft Report NUS-4531, EPRI Project RP2170-3, San Diego, CA: Electric Power Research Institute, 1984a.
6. Hannaman, G. W. & Spurgin, A. J. *Systematic Human Action Reliability Procedure (SHARP)*. EPRI NP-3583, Palo Alto, CA: Electric Power Research Institute, 1984b.
7. Hollnagel, E. Cognitive Reliability Error Analysis Method (CREAM), Oxford, UK: Elsevier, 1998.
8. International Atomic Energy Agency (IAEA), Human Error Classification and Data Collection, IAEA TECDOC 538, Vienna (A), 1990.
9. Institute of Nuclear Power Operations Group, *Building on the Principles for Enhancing Professionalism: Excellence in Human Performance,* Institute of Nuclear Power Operations*,* September, 1997.
10. International Nuclear Safety Advisory Group. *Safety Culture*, Safety Series No. 75-INSAG-4, International Atomic Energy Agency, 1991.
11. Kirwan, B., Kennedy, R., Taylor-Adams, S. and Lambert, B. *Validation of Three Human Reliability Assessment Techniques: THERP, HEART and JHEDI,* Volume I - Main Report, University of Birmingham, February 1994.
12. Macwan, A. and A. Mosleh. A. A Methodology for Modeling Operator Errors of Commission in a Probabilistic Risk Assessment. In *Reliability Engineering and System Safety*, Vol. 45, 139-157, 1994.
13. Organization for Economic Cooperation and Development (OECD) Nuclear Energy Agency (NEA). Critical Operator Actions - Human Reliability Modeling and Data Issues, Volume 1 and Appendix F (Questionnaire Responses). In *Final Task Report Prepared by Experts of the NEA Committee on the Safety of Nuclear Installations,*NEA/CSNI/98 (1), Principal Working Group No. 5, Task 94-1, Paris, France, February 1998.
14. Organization for Economic Cooperation and Development (OECD) Nuclear Energy Agency (NEA). *Nuclear Power Plant Operating Experiences from the IAEA/NEW Incident Reporting System, 1996-1999*, Paris, France, 2000.
15. Reason, J. *Human Error*, Cambridge, U.K.: Cambridge Univ. Press, 1990.
16. Reason, J. Managing the Risk of Organizational Accidents, Lincolnshire, UK Ashgate Press, 1997.
17. Spurgin, A. J., et. al. Operator Reliability Experiments (ORE) Using Power Plant Simulators, Vols 1 and 2: Executive Summary and Technical Report. EPRI-NP-6937, Electric Power Research Institute, Palo Alto, CA, 1990.
18. Public Services Electric and Gas Company, Salem Generating Station Individual Plant Examination (IPE), , 1993.
19. Commonwealth Edison, Quad Cities Response to Staff Evaluation Report and Modified Quad Cities Individual Plant Examination (IPE), 1996.

20. Standardized Plant Analysis Risk Model for Wolf Creek Generating Station (ASP PWR B), Revision 2QA, Idaho National Engineering and Environmental Laboratory, December 1997.
21. Strater, O. The Role of Plant Experience to Consider the Human Factor in Living PSA. In: H.P. Balfanz (Ed.*), 4th TUV-Workshop on Living PSA Applications in Hamburg*, TUV Nord, Hamburg, Germany, May 2-3, 1994.
22. Strater, O. *A Method for Human Reliability Data Collection and Assessment.* ESREL '96/PSAM-III, Crete, Greece, June 24-25, 1996.
23. Swain, A. D., and Guttmann, H.E. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (THERP) Final Report. NUREG/CR-1278, Washington, DC, 1983.
24. Swain, A.D. Accident Sequence Evaluation Program (ASEP) Human Reliability Analysis Procedure. NUREG/CR-4772, Washington, DC, 1987.
25. U.S. Nuclear Regulatory Commission. *Precursors to Potential Sever Core Damage Accidents: 1992, A Status Report*, Vol. 17–26, NUREG/CR-4674, Oak Ridge National Laboratory.
26. U.S. Nuclear Regulatory Commission. Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance, Summary Report, NUREG-1560, Vol. 1, Part 1B, October 1996.
27. U.S. Nuclear Regulatory Commission. An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis, Reg. Guide 1.174, July 1998.
28. U.S. Nuclear Regulatory Commission. *Recommendations for Reactor Oversight Process Improvement*, SECY-99-007, January 8, 1999.
29. U.S. Nuclear Regulatory Commission. Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA), NUREG-1624, Rev.1, May 2000.
30. Williams, J. C. A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance. In *Proceedings of the IEEE 4th Conference on Human Factors in Power Plants*, Monterey, California, June 6-9, 1988. New York: Institute of Electronic and Electrical Engineers, 1988.
31. Woods, D. D. Some Results on Operator Performance in Emergency Events, Institute of Chemical Engineers Symposium Series, 1984, 90, In *Ergonomics Problems in Process Operations*, Birmingham, U.K., 21-31, 11-13 July 1984.

APPENDIX A

QUANTITATIVE AND QUALITATIVE ANALYSES OF EVENTS

A1. Quantitatively Analyzed Events

The 23 operating events analyzed quantitatively are listed in Table A-1 and presented in this section. For each event, a synopsis summarizes the event history and insights from the LER or AIT. Following that, a table itemizes human performance issues for the event. The human errors that influenced the initiation, mitigation, or progression of the event ("active" errors), or that otherwise contributed to the event ("latent" errors) are described. The root cause of the event is listed where it was recorded in the LER or AIT report or easily determined by the analysis team.

Table A-1. Operating Events Analyzed Quantitatively.

Sect No.	Event Title	Date	LER or AIT Number
A1.1	ANO Unit 1 Event	May 19, 1996	LER 313-96005
A1.2	ANO Unit 2 Event	July 19, 1995	LER 368-95-001
A1.3	Beaver Valley Units 1 and 2 Event	October 12, 1993	LER 334-93-013
A1.4	Comanche Peak 1 Event	June 11, 1991	LERs 445-95-003 and 445-95-004
A1.5	D. C. Cook Event	September 12, 1995	LER 315-95-011
A1.6	Dresden Unit 3 Event	May 15, 1996	LER 249-96-004
A1.7	Haddam Neck Event	May 25 to June 27, 1993	LERs 213-93-006 and 213-93-007; AIT 93-080
A1.8	E. I. Hatch Unit 1 Event	January 26, 2000	LER 372-00-002
A1.9	Indian Point 2 Event	August 31, 1999	LER 247-99-015 and AIT 50-247/99-08
A1.10	LaSalle 1 Event	September 14, 1993	LER 373-93-015
A1.11	Limerick Event	September 11, 1995	LER 352-95-008
A1.12	McGuire 2 Event	December 27, 1993	LER 370-93-008
A1.13	Millstone 2 Event	January 25, 1995	LER 336-95-002
A1.14	Oconee Units 1, 2, and 3 Event	December 2, 1992	LER 269-92-018
A1.15	Oconee Nuclear Station, Unit 2, Docket 50-270		LER 270-97-001
A1.16	Oconee Unit 2	October 19, 1992	LER 270-92-004
A1.17	Perry Event	April 19, 1993	LER 440-93-011
A1.18	River Bend 1Event	September 8, 1994	LER 458-94-023

Sect No.	Event Title	Date	LER or AIT Number
A1.19	Robinson Events	July 8 to August 24, 1992	LERs 261-92-017, 261-92-013, and 261-92-018
A1.20	Seabrook Event	May 21, 1996	LER 443-96-003
A1.21	Sequoyah 1 and 2 Event	December 31, 1992	LER 327-92-027
A1.22	St. Lucie Unit 1 Event	October 27, 1997	LER 335-97-011
A1.23	Wolf Creek Generating Station Event	January 30, 1996	LER 482-96-001

A1.1 ANO Unit 1 Event, May 19, 1996 (LER 313-96-005)

Synopsis

On May 19, 1996, with Unit 1 at 100% power, a malfunction in the feedwater control circuitry caused a reactor scram. The malfunction, a common electrical fault that affected both 24-volt power supplies, caused a reduction in control oil pressure and a prompt corresponding reduction in the speed and output of main feed pump A. The insufficient heat removal by the feedwater system resulted in a high reactor pressure trip. Six of eight main steam safety valves on steam header B opened as designed on high reactor pressure. One valve failed to close. In accordance with procedures, the operators isolated steam generator B and allowed it to boil dry. Following the reactor trip, normal feedwater was lost because of further feedwater control deficiencies; the main feedwater pump B misinterpreted a demand signal increase and transferred into the diagnostic mode. It did not respond to the rapid feedwater reduction signal and remained at high speed. Because the train B feedwater block valves had closed, the main feedwater pump B tripped on high discharge pressure 14 seconds after reactor trip.

AIT Team Performance Insights

The licensee failed to respond to Information Notice 84-33 and other pertinent industry information relative to safety valve failures and failed cotter pins. The licensee also failed to respond to Information Notice 93-02, malfunction of a pressurizer code safety valve related to lock nut loosening on Crosby valves. Other evidence of inadequate assessment was the licensee's response to the Babcock and Wilcox (B&W) transient assessment program report CR3-94001, which discussed the failure of main steam safety valves to reseat because of cotter pin and release nut problems. The licensee assigned this issue a low priority for engineering review.

The AIT team found that a previous failure to reseat of a Unit 1 main steam safety valve was documented in LER 50-313/89-018. This safety valve failure was caused by the licensee's failure to install a release-nut cotter pin.

Information displayed in the control room during the transient was rendered inaccurate by unusable temperature sensors and problems with the safety parameter display system (SPDS). Problems with the SPDS had been noted as early as 1990 (CR-I-90-223). The licensee's corrective actions to resolve the deficiencies in the SPDS were deemed untimely. During the transient, operators had to manually calculate the tube-shell differential temperature.

Human Performance Issues

Description	Error Type	Error Subcategory
Operating with less-than-comprehensive testing of the new digital feedwater control system in the presence of system noise led to failure on demand.	Latent	Design change testing
Inadequate design of the feedwater control response for transient conditions caused wide speed changes (cycling) while in diagnostic mode.	Latent	Design deficiencies
The licensee delayed in acting on inspection findings and industry notices related to cotter pin and release nut problems with various safety valves.	Latent	Failure to respond to industry and internal notices
The licensee delayed in taking action in light of similar problem with main steam safety valve (MSSV).	Latent	Failure to trend and use problem reports
Operators were forced to perform calculations on the steam generator (SG) tube-to-shell differential temperature due to continuing operation with an inaccurate safety parameter display system.	Latent	Failure to correct known deficiencies
Operators were forced to perform work-arounds that made the transient more challenging. They had to manually operate an isolation valve instead of the atmospheric dump valve that failed due to binding.	Latent	Failure to correct known deficiencies
Ergonomic aspects of control room (CR) equipment contributed to operator workload and stress. SPDS was hard to read, and labeling of emergency plan notification form folders did not match the simulator.	Latent	Design deficiencies
The licensee continued operations in the presence of inadequate maintenance.	Latent	Management and Supervision

A1.2 ANO Unit 2 Event, July 19, 1995 (LER 368-95-001)

Synopsis

On July 19, 1995, during a Unit 2 procedure validation using the plant simulator, a condition was discovered in which failure of the green DC electrical bus could potentially render the red train of the emergency feedwater system inoperable. The failure would also render the green train, which is normally supplied from the green DC bus, inoperable. The trains for the emergency feedwater system, AC electrical power, and DC electrical power are designated as “red” and “green.” The emergency feedwater system is arranged in two trains, each of which can supply both steam generators. Each supply from the emergency feedwater pump to the steam generator has two motor-operated valves arranged in series. Two normally open valves - one in the line to each steam generator - in the emergency feedwater red train are powered from the green train of AC power and have a normally energized control relay that is powered from the green AC power.

The cause was a design error that occurred when electro-hydraulic valves were replaced with motor-operated valves. To ensure that emergency feedwater could be isolated on a main steam isolation signal, valves powered from the opposite AC power source were installed in each emergency feedwater flowpath. The design engineer's assumption that the AC-powered valves would stay "as-is" on a loss of power failed to consider the decay time of the voltage following a main generator trip.

Human Performance Issues

Description	Error Type	Error Subcategory
Human error occurred in the design of a plant modification that replaced electromechanical valves with motor operated valves.	Latent	Inadequate design Inadequate engineering evaluation
The design review process failed to discover the error.	Latent	Inadequate design review process
Testing of fielded systems was insufficient or inaccurate.	Latent	Inadequate design and design change testing

A1.3 Beaver Valley Units 1 and 2 Event, October 12, 1993 (LER 334-93-013)

Synopsis

On October 12, 1993, Unit 1 was operating at 100% power and Unit 2 was in a refueling outage with all fuel removed from the reactor vessel. At 1507 hours, Unit 1 experienced a large loss of offsite load when 10 offsite feed breakers in the Beaver Valley switchyard opened as a result of an inadvertent underfrequency system separation actuation. The load reduction caused the Unit 1 turbine to overspeed and trip, and resulted in a high flux rate reactor trip. The opening of the switchyard feed breakers and Unit 1 generator trip resulted in a LOOP to Units 1 and 2. Both Unit 1 emergency diesel generators (EDGs) and the required Unit 2 EDG started and supplied their required loads. The Unit 1 auxiliary feedwater system actuated due to low steam generator levels resulting from the reactor trip. Unit 1 was stabilized using emergency operating procedures. Following realignment of switchyard breakers, offsite power was restored to both units by 1522 hours.

On October 13, 1993, following a Unit 1 containment inspection, a reactor coolant system pressure boundary leak was discovered on the loop 1A cold leg vent valve RC-27. A Technical Specification– required cooldown was initiated, and Mode 5 was entered at 0304 hours on October 14, 1993.

The cause of the LOOP event was personnel error. A three-person electrical maintenance crew was performing scheduled outage maintenance on the Unit 2 main output breaker PCB 352. During verification of auxiliary contact alignment of the PCB 352 breaker, an inadvertent application of 125 V DC actuated an under-frequency separation scheme in the Beaver Valley switchyard. This resulted in the opening of seven 345-kV feed breakers (including Unit 1 main unit output breaker PCB 341) and three 138-kV feed breakers, and initiated the loss of electrical load at Unit 1.

Human Performance Issues

Description	Error Type	Error Subcategory
The licensee failed to update switchyard trip system based on plant electrical loading.	Latent	Design process
Personnel involved in maintenance activities incorrectly connected 125 V DC power using a multimeter.	Active	Maintenance practices
Facility operation department personnel were not included in switchyard work planning.	Latent	Command and control

A1.4 Comanche Peak 1 Event, June 11, 1995 (LERs 445-95-003 and 445-95-004)

Synopsis

On June 11, 1995, the Unit 1 balance-of-plant reactor operator (RO) (utility licensed) was performing the train A slave relay test for the K601A relay. During the test, a non–safety related inverter transferred from its normal inverter AC power supply to its bypass (alternate) AC power supply, which was de-energized per the slave relay test procedure. This resulted in loss of power to auxiliary relays 1-PY/2111 & 2112, which caused a main feedwater pump low oil pressure signal, tripping both condensate pumps. The loss of the condensate pumps resulted in a trip of both main feedwater pumps. A manual reactor trip was initiated due to the loss of feedwater to the steam generators.

Human Performance Issues

Description	Error Type	Error Subcategory
The system design failed to power trip relays for condensate pumps from different power sources.	Latent	Design deficiency
Inverter components were not calibrated.	Latent	Maintenance work package development, QA and use
The inverter for transient protection was inadequately designed.	Latent	Design deficiency
Governor valve experienced corrosion due to design factors.	Latent	Design deficiency
Maintenance failed to detect stem corrosion.	Latent	Maintenance work practices
Maintenance failed to detect water in the steam traps.	Latent	Maintenance work practices

A1.5 D.C. Cook Unit 1 Event, September 12, 1995 (LER 315-95-011)

Synopsis

On September 12, 1995, with Unit 1 defueled, the West centrifugal charging pump was started for a surveillance. The pump operated at full flow for 7 minutes before tripping. Investigation revealed that the pump had tripped on motor overcurrent due to an incorrect setting for a time overcurrent relay. The relay was recalibrated and returned to service.

The root cause of the event was a lack of re-qualification training leading to personnel error. The training program for relay calibration was reviewed, as was the calibration procedure.

The two instrumentation and control technicians involved were both trained and qualified within the plant relay training program. It was determined, however, that an excessive amount of time had elapsed between the original qualification of the technicians and the March 1995 relay calibration.

Human Performance Issues

Description	Error Type	Error Subcategory
Continuing training for instrument and control (I&C) technicians was inadequate for overcurrent relay setting.	Latent	Inadequate maintenance knowledge and training
Detail contained in the calibration procedure was inadequate.	Latent	Procedures and procedure development

A1.6 Dresden Unit 3 Event, May 15, 1996 (LER 249-96-004)

Synopsis

On May 15, 1996, while operating at 82% power, the Unit 3 experienced a failure of a feedwater regulating valve and subsequent reactor trip and emergency core cooling system actuation. Due to maintenance activities, the plant was operating with only a single FRV in service. The redundant FRV was isolated due to a steam leak that had been identified in September 1995. After the remaining FRV failed, all feedwater flow to the reactor was blocked and the water level rapidly dropped to the automatic low-level scram setpoint.

Control rods were fully inserted and all other equipment and isolation valves (main steam isolation valves and a recirculation sample isolation valve) opened unexpectedly during reset of Group 1 isolation. The operators manually re-closed the valves and re-verified that the other Group 1 primary containment isolation system (PCIS) valves had remained closed. An Unusual Event was declared, and the emergency plan was activated. The Unusual Event was terminated after the plant was in cold shutdown. The AIT report determined that the response to the event by operations, engineering, and plant support was good.

Human Performance Issues

Description	Error Type	Error Subcategory
The inspection frequency of the feed regulating valve was determined without technical basis.	Latent	Maintenance work practices
Lack of challenge for “not required” for review of generic failures.	Latent	Work package review
The plant was running with only one FRV operational.	Latent	Lack of technical understanding of defense in depth relationships Lack of risk basis understanding by plant personnel
The licensee delayed in placing FRV A back in service promptly.	Latent	Maintenance work process prioritization, planning, scheduling Misunderstanding the impact of it not being in service (technical knowledge factor)
The PCIS relay failed.	Latent	Lack of trending on relay repair information across previous years

Description	Error Type	Error Subcategory
		Organizational learning factor
Industry practices were not followed.	Latent	Lack of corrective action infrastructure to change the procedure to place control switches in the closed position before resetting Group 1 isolation

A1.7 Haddam Neck Event, May 25 to June 27, 1993 (LERs 213-93-006 and 213-93-007 and AIT 93-080)

Synopsis

On June 24, 1993, the plant was shut down. During breaker failure trip logic testing on the offsite power tiebreaker, the station experienced a total loss of offsite power. In response to the loss of offsite power, both EDGs automatically started and provided emergency power to the station. The plant was in cold shutdown at the time of the event and shutdown cooling was temporarily lost. The root cause for this event has been identified as a wiring error in the offsite power tiebreaker failure trip logic. The wiring error occurred during or shortly following plant construction. The wiring error had not been previously identified since this was the first test conducted of this particular trip logic that included tripping the breakers.

Three related occurrences were involved in this event. On May 25, 1993, it was discovered that the air receiver pressure for the PORVs decayed faster than allowed by Technical Specifications. On June 26, 1993, during surveillance testing of train A of the safety injection actuation logic with a partial loss of offsite power, a complete loss of offsite power occurred. On June 27, 1993, during surveillance testing of train B of the safety injection actuation logic with a partial loss of offsite power, a temporary loss of a motor control center (MCC) occurred when the automatic bus transfer scheme failed to operate.

Human Performance Issues

Loss of off-site power

Description	Error Type	Error Subcategory
An operator failed to reset safety injection lock-in relays when restoring safety injection.	Latent	Incorrect operator action
An operator failed to identify a failure based on abnormal indications of voltage during earlier outage activities.	Latent	Failure to fully investigate Attributing failure to wrong component (technical knowledge) Improper engineering evaluation
Some operations and maintenance personnel believed there was a problem with a voltage switch when an actual problem did not exist. This may have led personnel to believe that the failure source was the switch and not a fuse.	Latent	Training. Reliance on unverified information
Wiring of the breaker was incorrect.	Latent	Configuration management/ drawing control

Loss of MCC 5

Description	Error Type	Error Subcategory
An improper classification of the emergency was transmitted.	Latent	Operator knowledge and training
The investigation by licensee failed to identify the breaker that had failed during initial investigation.	Latent	Engineering evaluation
The manufacturer of the breakers failed to incorporate information in vendor manuals even though information was incorporated in another breaker manual that used identical relays.	Latent	Vendor manual configuration control
There was a failure to determine a positive root cause for previous failures of the same relay.	Latent	Incomplete engineering analysis
The snap ring for the breakers was improperly installed.	Latent	Maintenance practices

EDG Failure During 24-Hour Run

Description	Error Type	Error Subcategory
Adequate cleanliness of equipment was not maintained.	Latent	Maintenance practices
Long-term capabilities of equipment (e.g., cooling systems) were not considered.	Latent	Engineering evaluation
There was insufficient consideration of aging components in an environment with inadequate cooling.	Latent	Engineering evaluation i.e., plant aging analysis not conducted

PORV failure

Description	Error Type	Error Subcategory
An improper valve lineup prevented monitoring moisture content in the air system, which would have allowed for early detection and correction of the problem.	Latent	Incorrect operator action

A1.8 E.I. Hatch Unit 1 Event, January 26, 2000 (LER 372-00-002)

Synopsis

On January 26, 2000, Unit 1 was at 100% of rated power when the reactor shut down automatically and the Group 2 primary containment isolation valves (PCIVs) closed on low water level. The water level decreased when feedwater flow was reduced by the unexpected closure of an inlet valve to a feedwater heater. Following shutdown, water level continued to decrease due to void collapse from the rapid reduction in power, resulting in closure of the Group 5 PCIVs and automatic initiation of the reactor core isolation cooling (RCIC) and high-pressure coolant injection (HPCI) systems. Water level reached a minimum of 54 in. below instrument zero. The reactor feedwater pumps, RCIC, HPCI, and control rod drive systems restored water level to >40 in. above instrument zero within 40 seconds of the shutdown.

Human Performance Issues

Description	Error Type	Error Subcategory
Industry notices for GE Control switches used to position inlet valves were not implemented.	Latent	Failure to respond to industry notices
Operators failed to observe automatic flow demand before transferring HPCI control from manual back to automatic.	Active	Operator action/inaction
Operators failed to fully recognize impact of plant conditions on control room indications.	Active	Operator knowledge and training
RCIC restart procedures were inadequate.	Latent	Procedures and procedures development
RCIC restart training was inadequate.	Latent	Operator knowledge and training
Confusion during shift turnover resulted in unclear lines of responsibility and subsequent difficulties causing delays in identifying that HPCI did not immediately trip at the high-level setpoint and closure of main steam isolation valves (MSIVs).	Active	Command and control
The SRV position indication was inadequately designed to provide proper indication when the SRV is passing a steam-water mixture.	Latent	Design deficiency - ergonomics

A1.9 Indian Point 2 Event, August 31, 1999 LER 247-99-015 and AIT 50-247/99-08)

Synopsis

On August 31, 1999, at 2:31 p.m., the Unit 2 reactor automatically tripped while at 99% power. The reactor protection system (RPS) trip indication was over-temperature delta-temperature (OT?T). The cause of the RPS trip was a spurious signal to one channel of the OT?T instrumentation while another channel was being tested and was in a trip condition. When any two of the four channels are in a trip condition, the RPS will cause a reactor trip. Incorrect electrical equipment lineups and electrical equipment failure resulted in a loss of vital AC, vital DC and instrument AC power.

Human Performance Issues

Description	Error Type	Error Subcategory
The station auxiliary transformer load tap changer was not maintained in the automatic position as required by the licensing bases.	Latent	Configuration management (Inadequate knowledge of regulatory requirements and safety design basis)
The 23 EDG output breaker over-current setpoint was not properly controlled due to an inadequate test methodology.	Latent	Configuration management. Secondarily, inadequate post maintenance Test process
The 23 EDG load sequencing had been changed and, within relay tolerances, allowed multiple pump motors to load onto the bus at one time.	Latent	Inadequate design change testing — failure to consider blackout loading sequence

Description	Error Type	Error Subcategory
The degraded voltage relay reset values for the 480 V buses were not controlled.	Latent	Configuration management
Station managers did not anticipate the plant vulnerabilities caused by the partial loss of power, nor did they establish priorities for recovery over shutdown.	Latent	Supervisory knowledge and training
Incorrect electrical line-up.	Latent	Maintenance and maintenance practices
Station supervision did not ensure that the plant staff responded to assist the operators to mitigate the degraded plant conditions as quickly as possible.	Active	Command and control
Equipment restoration plans and contingency planning were not clearly understood or fully developed.	Latent	Supervisory communication
Engineering personnel did not investigate the cause of an OT?T signal increase that had occurred on August 26, 1999.	Latent	Operator knowledge and training
Station personnel failed to recognize and evaluate a potential trend in RPS problems and failures.	Latent	Failure to trend and use problem reports
Work control personnel were not notified of the spurious trips in the OT?T circuitry for consideration in work planning.	Latent	Communications
Station personnel missed an earlier opportunity to identify the Amptector test methodology problem.	Latent	Failure to correct known deficiencies
Corrective actions for previous breaker problems, which addressed test methodology, were overdue and incomplete.	Latent	Failure to correct known deficiencies.
Station personnel did not evaluate the station auxiliary transformer load tap changer condition report for safety and operability impacts.	Latent	Engineering review and analysis deficiency
Procedures had not been implemented to reflect the required operational mode of the load tap changer for compliance with the plant design basis.	Latent	Procedures and procedural implementation
Entry into TS limiting conditions for operations (LCOs) was late.	Active	Inadequate operator technical knowledge and training
Recovery actions were poorly coordinated.	Active	Command and control and resource allocation

Description	Error Type	Error Subcategory
The emergency plan failed to provide adequate information for declaring an unusual event unless off-site power was unavailable.	Latent	Procedures and procedural deficiencies.
The daily risk factors calculated by the watch engineer were 5.6 x 10-3 and were communicated to the shift manager and discussed with crew, but the risk information was not communicated to senior management. The risk information was not used to expedite recovery actions or equipment repairs.	Active	Communications
Technical support was not timely to minimize time in degraded conditions with high risk-significant failures (i.e., 10 hours to tag and take ground measurements on 6A bus).	Active	Resource allocation
Notification procedures for state and local agencies were inconsistent and unclear.	Latent	Inadequate procedures
The required mode change missed completion by failing to be less than 350ºF within 12 hours.	Active	Communications: Shift turnover failed to list all applicable LCOs

A1.10 LaSalle 1 Event, September 14, 1993 (LER 373-93-015)

Synopsis

On September 14, 1993, Unit 1 was at 100% power. Following a fault on the station auxiliary transformer (SAT), the reactor scrammed due to low water level. No surveillance or other activities were in progress.

Following a fault on the station auxiliary transformer (SAT), the reactor scrammed due to low water level. The turbine subsequently tripped automatically. The loss of power affected operations through significant equipment problems [i.e., SRVs exhibited anomalies, RPS Bus 1B lost, RPS motor generator (MG) set drive motor shorted, service water, instrument air, and shutdown cooling system unable to function (due to containment isolation)]. The loss of RPS Bus 1B also caused the security secondary alarm station and heating, ventilation, and air conditioning (HVAC) to the prime security computer and service air systems to malfunction.

The bus duct design did not provide drainage paths for accumulated moisture. Spent fuel cooling of both units was lost when a Unit 1 panel was lost. Air compressors needed two power sources to operate. No cross-tie was available for backup power supply of RPS buses to Unit 2.

The AIT 50-373/374 source document dated October 1993 noted the following: Inadequate maintenance resulted in several equipment failures that occurred during the event and recovery. The most probable cause of SAT trip was inadequate maintenance. The inspection team noted that inadequate maintenance has been a contributing factor to other events at LaSalle and previous corrective actions had not been effective. Strengths in responding to the event included operating crew and technical support center personnel actions to deal with the event and support provided by other Commonwealth Edison organizations. This included sound command and control in the control room and use of extra available personnel. In general, the operators exhibited excellent coordination and teamwork.

Emergency lighting was insufficient for operation of some chiller valves during the loss of power, and jumpers should have been made available with abnormal procedures for loss of power in the manner that they were for emergency operating procedures (EOPs). The AIT concluded that initiation of the event itself was due to deficiencies in the maintenance work process, including corrective actions, technical knowledge, attention to detail, and organizational learning (failure to learn from a previous event in August of 1992).

Human Performance Issues

Loss of SAT

Description	Error Type	Error Subcategory
Licensee maintenance practices allowed for corrosion build-up on the lower portion of SAT duct.	Latent	Inadequate preventive/corrective maintenance practices
Procedures were lacking to backfeed the 6.9-kV buses via the unit auxiliary transformer (UAT) resulting in the 29 hours required to initiate back feeding. The AIT team concluded that normal backfeed procedures took from 8 to 16 hours.	Latent	Procedures
Licensee maintenance practices allowed for corrosion build up in the surge suppressor compartment.	Latent	Inadequate maintenance practices including inadequate inspection
The duct design did not allow for proper drainage.	Latent	Design deficiency
Overall inadequate design and inappropriate maintenance were compounded by failure of the corrective action program in response to a previous plant event.	Latent	Corrective action program (failure to correct known deficiencies)

SRV Anomalies

Description	Error Type	Error Subcategory
The solenoid air valve to actuator body leak reduced air pressure below that required to operate the SRV.	Latent	Maintenance work practices

Loss of RPS Bus 1B

Description	Error Type	Error Subcategory
Layers of dirt were not detected on motor windings during inspections. Layers of dirt were not detected on motor windings during inspections.	Latent	Maintenance work practices Knowledge
Degradation of insulation occurred on motor generator set.	Latent	Maintenance work practices. Coupled with Failure to correct known deficiencies

A1.11 Limerick Unit 1 Event, September 11, 1995 (LER 352-95-008)

Synopsis

On September 11, 1995, Unit 1 was manually shut down in response to the unexpected opening of the 'M' main steam SRV when the valve could not be closed within 2 minutes per TS. Following the reactor shutdown, the TS maximum reactor coolant system (RCS) cool-down rate of 100ºF/hour was temporarily exceeded due to the RCS depressurization through the open SRV. Inspection of the SRV revealed steam erosion attributed to pilot valve seat leakage that resulted in the failure of the pilot valve.

Human Performance Issues

Description	Error Type	Error Subcategory
Material control during maintenance activities performed in the containment was inadequate.	Latent	Maintenance work process
Management failed to set cleanliness expectations for the containment and suppression pool.	Latent	Inadequate management supervision and controls
Personnel were not sufficiently sensitive to effects of cleanliness on ECCS operability.	Latent	Lack of maintenance technical knowledge

A1.12 McGuire 2 Event, December 27, 1993 (LER 370-93-008)

Synopsis

On December 27, 1993, Unit 2 was operating at 100% power when an electrical insulator in the 525 kV switchyard failed. This caused one of the two paths feeding the switchyard from the main generator to isolate. The main generator failed to run back as designed and the second offsite path isolated on overcurrent, resulting in a loss of offsite power to the plant. The electrical transient caused a reactor trip and turbine trip.

Human Performance Issues

Description	Error Type	Error Subcategory
Licensee did not appear to understand the switchyard relay protection scheme, thereby allowing a design to exist that placed undue reliance on proper functioning of a non-safety related turbine runback feature.	Latent	Inadequate operations knowledge and training
There was no testing program for the turbine runback feature, which might have identified the potential design and configuration problems.	Latent	Inadequate test process
Maintenance and testing procedures for the MSIVs failed to incorporate vendor recommendations.	Latent	Failure to follow industry-recommended practices
There was no post-modification testing on the MSIV after a modification removed additional closing force by air pressure. There was a failure to detect a significant change in the valve's performance.	Latent	Inadequate test process

Description	Error Type	Error Subcategory
Excessive time was taken to read the EOP fold-out pages, delaying the implementation of procedural steps to isolate MSIVs prior to a safety injection (SI) signal. This deficiency had been identified previously.	Active	Failure to correct known deficiency
The shift supervisor (SS) acted as EOP reader for approximately 15 minutes, which reduced the supervisor's ability to oversee the event.	Active	Command and control
The duties and responsibilities of the SROs during an emergency are not clearly defined.	Latent	Command and control
Instrumentation and electrical personnel took actions, on their own initiative, without procedural direction and without use of reference material (i.e., CR drawings) that opened the isolated MSIV upsteam drain lines.	Active	Incorrect operator actions
Operators did not recall that the drain valves had been modified, changing their fail-safe position from open to closed on loss of power. Operators relied on past experience and simulator training rather than training that emphasized the modifications.	Latent	Inadequate training
Control room drawings and instrument details did not clearly and unambiguously identify instrument modifications and could have led to confusion and delay.	Latent	Configuration management
Local operation of some valves during loss of electrical power (required by procedures) may be difficult or error prone because of inadequate lighting, access, and labeling.	Latent	Design deficiency - ergonomics
Operators did not perform the licensee notification procedure, resulting in an inaccurate and incomplete report of the event.	Active	Incorrect operator action/inaction
The licensee failed to evaluate actions during a previous LOOP and create procedures to mitigate the main steam isolation and SI prior to their occurring.	Latent	Failure to correct know deficiencies

A1.13 Millstone 2 Event, January 25, 1995 (LER 336-95-002)

Synopsis

On January 25, 1995, with Unit 2 defueled, an engineering evaluation confirmed that the assumptions made for the original design basis analysis for the containment sump isolation valves were non-conservative with respect to the maximum calculated forces that would be required to open the valves. The engineering evaluation determined that these valves are potentially susceptible to a pressure-locking phenomenon that might preclude them from performing their safety-related function during a postulated design-basis accident condition. The valves had been analyzed previously for pressure locking, but that evaluation, performed in 1989, failed to recognize the valves' susceptibility to pressure locking. The valves were declared inoperable.

Human Performance Issues

Description	Error Type	Error Subcategory
Inadequate engineering evaluation of valve susceptibility to pressure locking and thermal binding allowed for a common mode failure that would prevent entry into containment sump recirculation mode.	Latent	Engineering evaluation and review process
The utility's acceptance of the analysis performed by the first vendor was not stringent enough.	Latent	Management supervision

A1.14 Oconee Units 1, 2, and 3 Event, December 2, 1992 (LER 269-92-018)

Synopsis

On December 2, 1992, Units 1, 2 and 3 were operating at 100% power. During the annual emergency testing of the Keowee hydroelectric station units, one of the output breakers could not be manually closed.

The Keowee emergency power system consists of two hydroelectric generators that provide an emergency onsite power source for the Oconee Nuclear Station via two separate and independent paths.

Human Performance Issues

Description	Error Type	Error Subcategory
The licensee failed to consider the interaction between systems or components (i.e., low DC voltage combined with limited time for energizing the closing coil).	Latent	Engineering evaluation
The system was not designed to ensure operation with the minimum values for the input voltages.	Latent	Design deficiency
A replacement component, i.e. relay, was not tested under both operating modes.	Latent	Test development process
The inspection created a voltage regulator ground.	Active	Maintenance practice
The work package implemented a deficient pump scheme change. The work package also failed to document calculations that were employed.	Latent	Work package development, QA and use

A1.15 Oconee Nuclear Station Unit 2, Docket 50-270 (LER 270-97-001)

Synopsis

On April 21, 1997, at approximately 2245 hours, Unit 2 was operating at 100% power when the operators noted indications of a 2.5 gpm RCS leak. The leakage source could not be identified, as required by technical specifications. The unit was shutdown within 24 hour as required by technical specifications. Leakage increased to greater than 10 gpm before decreasing due to the cooldown. A Notification of Unusual Event (NOUE) was declared due to leakage exceeding 10 gpm. Similar problems with thermal sleeves and safe ends had been experienced in 1982 at Crystal River 3 and Oconee, and in 1988 at Farley 2 and Davis Besse.

Human Performance Issues

Description	Error Type	Error Subcategory
An effective HPI nozzle inspection program based on available industry recommendations was not implemented.	Latent	Failure to respond to industry an internal notices
There was a failure to effectively address known problems and implement appropriate corrective actions.	Latent	Failure to correct known deficiencies
There was inadequate consideration of the effect of thermal stress on nozzles.	Latent	Engineering design review process not outwardly focused to incorporate industry findings
Plant operations were not managed to minimize thermal stresses.	Latent	Management and supervision
Ultrasonic testing (UT) testing as scoped was not thorough enough to identify these problems.	Latent	Failure to follow industry practices.
Evaluation and interpretation of radiographic testing (RT) test results was inadequate.	Latent	Flawed nondestructive examination and review practices

A1.16 Oconee 2 Event of October 19, 1992 (LER 270-92-004)

Synopsis

On October 19, 1992, while Unit 2 was at 100% power with no significant concurrent equipment problems, maintenance was in progress to replace one of the 230kV switching station batteries. The Oconee Unit 1 supervisor was present at the switchyard relay house to perform switch alignments. The supervisor locally opens the crosstie breaker between two busses in the 230-kV switchyard in accordance with existing procedure. A routine fire drill was occurring in another building, and the Unit 2 supervisor and several auxiliary operators were involved in that drill. The Unit 3 supervisor was present in the Unit 1/Unit 2-control room. Keowee Unit 1 (a hydro generator supplied by Lake Keowee) was operating and available to supply the overhead emergency power path. Keowee Unit 2 was operable and aligned to the underground emergency power path. Transformer CT-5 was energized and available to manually supply the standby busses from the central switchyard.

A DC control power problem in the 230-kV switchyard resulting from a D.C. voltage surge caused a bus lockout and subsequent switchyard isolation. This lockout caused a Unit 2 main generator transformer lockout. Unit 2 transformer breakers were also opened by the lockout, and AC power was restored to the units from the Keowee hydro-station. Unit 1 and 3 continued generating. Next, off-site power to Unit 1 and Unit 3 startup transformers was lost.

After Keowee Unit 1 separated from the grid, it oversped and a normal generator lockout was received. The hydro-station busses fast transferred to an alternate power source, as design. Switchyard isolation temporarily de-energized the overhead path, and both Keowee emergency units started. These emergency start signs overrode the Keowee Unit 1 normal generator lockout.

The Oconee Unit 2 main generator transformer lockout produced a turbine and reactor trip. Oconee Unit 2 main feed breakers (MFBs) were de-energized due to the trip and were not automatically re-energized from the startup transformer due to the switchyard busses being locked out. Oconee Unit 2 RCPs tripped due to loss of power and then went into natural circulation. Oconee Unit 2 condensate and feedwater pumps were lost when the MFBs were de-energized. Loss of Oconee Unit 2 MFB also de-energized the battery charger SY-2. Main condenser cooling was provided by gravity flow as designed.

Human Performance Issues

Description	Error Type	Error Subcategory
Accident analysis planning did not fully envelop the extent of Keowee hydroelectric station's critical role in terms of mitigation and recovery. Deficient planning and emergency response work process lead to inadequate procedures.	Latent	Procedures and procedures development.
The work package placed the battery charger in a line-up without the battery connected, which is outside the design capabilities of the charger.	Latent	Work package development, QA and use
The plant organization failed to prioritize correcting a Zener diode deficiency as identified by Westinghouse. Duke Engineering had determined this repair to be required for Oconee.	Latent	Failure to respond to industry and internal reports
Procedures were not fully developed to support handling of the event; Keowee operators had no	Latent	Procedures and procedures development

Description	Error Type	Error Subcategory
specific procedure for responding to, or verifying, emergency start of the Keowee hydro units.		
Keowee auxiliary load center automatic transfer circuitry had several deficiencies that lead to loss of telephone and alarm annunciation indications.	Latent	Design deficiencies
Keowee operators demonstrated a lack of knowledge in how to respond to their control room annunciation of abnormal conditions.	Latent	Training and knowledge
The AIT team concluded that the live bus transfer procedure was inadequate. Training for that procedure was also inadequate.	Latent	Procedures
Oconee Unit 2 procedures did not require verification of the proper operation of the Keowee hydro generators from either the available Oconee indications or the on-shift Keowee operators.	Latent	Procedures and procedures development
No guidance existed in procedures for recovery from an improper lineup.	Latent	Procedure and procedures development

Description	Error Type	Error Subcategory
Oconee management were not aware of the “de-energized/overheat-feeder-interlock” feature (Unit 2 trips when Unit 1 is shutdown because no voltage is present on the overhead path). This resulted in an inadvertent loss of both Keowee units during the recovery phase.	Latent	Management lack of systems and technical understanding
Oconee control room staff were not aware of the “de-energized/overheat-feeder-interlock” feature that could potentially trip Unit 2 when Unit 1 is shut down.	Latent	Operator lack of technical understanding
The level and significance of problems at Keowee during the event were not fully communicated or understood.	Active	Communications
The loss of phone communications contributed to delays in responding to events.	Active	Communications
Keowee annunciator and computer alarm printers were lost when auxiliary buses supplying power failed.	Active	Ineffective indication of abnormal conditions.
A complex and atypical design for the emergency power system and interacting systems contributed to problems operating these systems.	Latent	Design deficiencies.
The battery charger was not adequately sized to replace the battery in the existing configuration.	Latent	Work package development and QA should have specified correct battery size.
There was a lack of rigor in operating the DC power system, which functions as a safety system.	Active	Maintenance practices
An MG-6 relay at Keowee failed due to excessive resistance; a similar problem had been identified in December 1992.	Latent	Failure to identify by trending and use of problem reports
Keowee took actions without concurrence or direction from Oconee control room, even through the actions had an impact on the Oconee emergency power.	Latent	Command and control
Keowee lacked emergency procedures for this and other similar sequences.	Latent	Procedures and procedures development

A1.17 Perry Event, April 19, 1993 (LER 440-93-011)

Synopsis

On April 19, 1993, an engineering evaluation determined that excessive strainer differential pressure across the residual heat removal (RHR) suction strainers could have compromised long-term cooling during and following 100 days of continuous post-LOCA operation.

Human Performance Issues

Description	Error Type	Error Subcategory
The licensee's inspection processes failed to identify a problem during previous inspections.	Latent	Inadequate maintenance practices
Material control during maintenance activities in the containment was inadequate.	Latent	Inadequate maintenance practices
Management failed to set cleanliness expectations for the containment and suppression pool.	Latent	Inadequate management controls
Personnel sensitivity to effects of cleanliness on ECCS operability was inadequate.	Latent	Lack of system knowledge Situational awareness

A1.18 River Bend Event, September 8, 1994 (LER 458-94-023)

Synopsis

On September 8, 1994, the plant was at 97% power when an automatic reactor scram occurred due to a false high reactor water level condition, sensed by the C and D channels of the narrow range reactor water level instrumentation. The control room operators had no indication of the origin of the scram at the time it occurred. There was no control room indication of a reactor water level increase or a feedwater level excursion. Operators initiated recovery procedures.

Human Performance Issues

Description	Error Type	Error Subcategory
Maintenance work instructions for establishing damping for Rosemount transmitters were inadequate.	Latent	Work package development, QA and use
Engineering allowed other maintenance processes to negate the Rosemount transmitter damping.	Latent	Inadequate engineering evaluation
Operator knowledge of main turbine/generator operation was weak.	Latent	Operator training
Operator communications both within the operating crew and outside departments were weak, resulting in operating outside EOP bands and missing a surveillance required by technical specifications.	Latent	Communications
Maintenance on the RCIC turbine governor valve was improper due to installation of incorrect washers.	Latent	Maintenance practices
Technical specification limits established for chemistry could not be physically attained within the allowable time.	Latent	Configuration management. Maintenance of design basis documents
Miscalibration of reverse power relays prevented turbine generator trip.	Latent	Maintenance practices

A1.19 Robinson Events, July 8–August 24, 1992 (LERs 261-92-017, 261-92-013, and 261-92-018)

Synopsis

On July 8, 1992, the “B” SI pump was declared out of service because of low flow on the pump’s recirculation line. Plastic sheet material was found in the B SI pump minimum flowline. The plastic material was believed to be from a purge dam that had been fabricated for welding operations for a modification to the minimum flow line for the RHR system during the cycle 14 refueling outage.

On August 22, 1992, with the plant at 100% power, a LOOP occurred because of the loss of the startup transformer. On August 24, 1992, following the LOOP and before plant restart, the B SI pump was tested and declared inoperable because of low flow in the recirculation line.

The “A” SI pump was also declared inoperable because of reduced flow in its recirculation line.

Human Performance Issues

Description	Error Type	Error Subcategory
Debris from failed dams was not removed. Concern and action for debris in system connection to the RCS were inadequate.	Latent	Inadequate technical knowledge
QA requirements were inadequate to ensure maintenance of system cleanliness.	Latent	Maintenance practices
Improper operation and/or maintenance caused the junction box to be rotated to a position that did not allow for proper drainage.	Latent	Maintenance practices
The junction box was improperly designed; it did not include necessary fasteners to assure that it remained in an orientation that allowed for drainage.	Latent	Design deficiency

A1.20 Seabrook Event, May 21, 1996 (LER 443-96-003)

Synopsis

On May 21, 1996, the turbine-driven emergency feedwater pump (FW-P-37A) was started in support of quarterly surveillance testing. During the performance of this testing sparks were observed emanating from the outboard mechanical seal area.

Human Performance Issues

Description	Error Type	Error Subcategory
Design of turbine driven emergency feedwater pump seals required use of non-standard maintenance practices for seal installation.	Latent	Design deficiency
The procedure for seal replacement did not include the requirement to use a dial indicator.	Latent	Procedures and procedural development.
Previous problems with seal failures were not effectively captured for use by individuals involved in future seal replacement.	Latent	Failure to trend and use problem reports

Description	Error Type	Error Subcategory
Lessons learned were not incorporated into maintenance procedures.	Latent	Work package development QA, and use

A1.21 Sequoyah 1 and 2 Event, December 31, 1992 (LER 327-92-027)

Synopsis

On December 31, 1992, Units 1 and 2 were operating at 100% power. Both units received a reactor trip signal because of reactor pump bus undervoltage. The undervoltage condition resulted from an internal fault in a new switchyard power circuit breaker that had been in service approximately 11 minutes.

The operating staff for both units performed EOPs for the plant conditions. The Unit 1 operating crew consisted of an SRO and two ROs, and the Unit 2 operating crew consisted of an SRO and one RO. The crew staffing, although meeting the technical specification requirements, was one less than normal due to an operator calling in sick. Management decided against calling in a replacement operator.

Following an automatic initiation of the AFW system, excessive RCS cooldown may occur if the AFW is not throttled in a timely manner. Reducing RCS temperature below 540ºF requires initiating emergency boration. The crew initiated boration using the normal lineup instead of the emergency boration flowpath. This incorrect action resulted in the coolant charging pumps operating for approximately one minute without a suction source. Incorrect switch positions resulted in additional equipment failing to respond as required for plant conditions.

Human Performance Issues

Description	Error Type	Error Subcategory
Insufficient staffing to respond to a dual plant trip resulted in excessive cooldown of the RCS.	Active	Command and control and resource allocation. Shift supervisor decided not to call in an operator.
An operator failed to read, and thus perform, the correct procedure.	Active	Operator action/inaction
Control switches were in incorrect positions, preventing automatic actions from occurring.	Latent	Configuration management of equipment
Inappropriate testing methodology was used for power circuit breakers.	Latent	Inadequate post-maintenance testing
Operators failed to manually perform the actions that failed to occur automatically.	Active	Operator actions
Operators failed to understand the impact system lineups would have on ongoing evolutions.	Active	Knowledge and Training
The testing methodology failed to appropriately assess potential risks involved, and failed to evaluate alternative testing methodologies.	Latent	Workpackage QA, and development.
Inadequate communication existed between work organizations responsible for assessing the risks associated with breaker testing.	Latent	Communications

Description	Error Type	Error Subcategory
Test documentation lacked sufficient detail for site management to understand the potential risks of the testing.	Latent	Work package development
Breaker testing procedures failed to prevent conditions that would cause breaker failure.	Latent	Testing procedure development

A1.22 St. Lucie Unit 1 Event, October 27, 1997 (LER 335-97-011)

Synopsis

On October 27, 1997, Unit 1 was defueled in support of the steam generator replacement refueling outage. During the outage, obsolete engineered safety features actuation system (ESFAS) bistables were replaced to improve system reliability and calibration methods. The equipment replacement included all four channels of refueling water tank (RWT) low level bistables. A low RWT level initiates the recirculation actuation signal (RAS), which shifts the suction for the safety injection systems from the RWT to the containment sump during LOCA.

Human Performance Issues

Description	Error Type	Error Subcategory
The engineering process for the set point and loop scaling process was inadequate.	Latent	Engineering evaluation and review
Configuration management controls during instrumentation changes were inadequate.	Latent	Configuration management
Procedural changes for instruments were inadequate.	Latent	Procedures and procedures development
Communications between all departments involved with a set point change were ineffective.	Latent	Communications
The organizational structure placed responsibility for fully implementing changes across multiple organizations.	Latent	Organizational structure
The testing process lacked an independent method for verifying that bistable setpoints occurred at expected level indications.	Latent	Design change testing
The change process lacked cross-checks.	Latent	Design change testing

A1.23 Wolf Creek Generating Station Event, January 30, 1996 (LER 482-96-001)

Synopsis

On January 30, 1996, the plant was operating at 98% power. Circulation water alarms were received in the control room. Investigation indicated increased differential pressure across the traveling screens caused by freezing of the traveling screens.

Post trip, the turbine-drive auxiliary feedwater (TDAFW) pump was reported to have excessive seal leakage, which was caused by the inboard seal packing failure. The TDAFW pump was declared inoperable and the motor-driven auxiliary feedwater pump was used to maintain steam generator levels.

The cause for the loss of level in the essential service water system (ESWS) suction bays was the buildup of Frazil ice on the trash racks on the inlet to the bay. The Frazil ice was only discovered after divers inspected the trash racks.

Human Performance Issues

Description	Error Type	Error Subcategory
The incorrect lineup of the ESWS was not corrected after it was identified.	Active	Operator action
An unfamiliar evolution for ESWS was performed without using a procedure or having a second operator verify the lineup using the procedure.	Active	Command and control
Knowledge and training for the conditions that will cause Frazil icing and the effects of Frazil icing were inadequate.	Latent	Lack of training
The design of warming lines was inadequate.	Latent	Design deficiency
Procedures to identify and respond to Frazil icing in the trash racks were lacking.	Latent	Procedural control
A technical specification interpretation previously had indicated, incorrectly, that Frazil icing conditions could not occur in the ESW pump house due to its being enclosed and heated.	Latent	Engineering evaluation and review
Information transfer concerning the status of the ultimate heat sink was inadequate.	Active	Inadequate communications
Equipment failed due to a seal leak caused by failed packing.	Latent	Maintenance practices
Equipment was declared operable without adequate engineering evaluation or determination of the root cause for the failure.	Active	Engineering evaluation and review
There was a delay in performing cooldown to comply with technical specification time requirements.	Active	Operator actions

A2. Qualitatively Analyzed Events

Qualitative analyses were performed on 14 significant events for which SPAR models were not available. Summaries of those events are listed in Table A2-1 and presented in this section. For each, a synopsis summarizes the event history and insights from the LER or AIT. Following that, a table itemizes human performance issues for the event. The human actions or errors that influenced the initiation, mitigation, or progression of the event (“active” errors) or that otherwise contributed to the event (“latent” errors) are described. The root cause of the event is listed where it was recorded in the LER or AIT report.

Table A-2. Operating Events Analyzed Qualitatively.

Sect. No.	Event Title	Date	LER or AIT Number
A2.1	Byron 1 Event	May 23, 1996	LER 454-96-007
A2.2	Callaway Event	October 17, 1992	LER 483-92-011
A2.3	Calvert Cliffs 2 Event	January 12, 1994	LER 318-94-001
A2.4	Catawba 1 & 2 Event	February 23, 1993	LER 413-93-002
A2.5	Catawba 2 Event	February 6, 1996	LER 414-96-001
A2.6	Fort Calhoun Unit 1 Event	July 3, 1992	LER 285-92-023
A2.7	Oconee 2 Event	May 3, 1997	LER 287-97-003
A2.8	Oyster Creek Event	May 3, 1992	LER 219-92-005
A2.9	Point Beach 1 Event	February 7, 1994	LER 266-94-002
A2.10	Quad Cities Event	April 22, 1993	LER 265-93-010
A2.11	Salem 1 Event	April 7, 1994	LER 272-94-007
A2.12	South Texas Project Event	December 29, 1992, to January 22, 1993	LERs 498-93-005 and 498-93-007
A2.13	Turkey Point Conditions since Initial Licensing	1984–1992	LER 250-92-001
A2.14	Wolf Creek Generating Station Generating Station, Docket 50-482	September 17, 1994	LER 482-94-013

A2.1 Byron 1 Event, May 23, 1996 (LER 454-96-007)

Synopsis

On May 23, 1996, Unit 1 was in cold shutdown and Unit 2 was at 100% power when a LOOP occurred due to a trip of the Unit 1 SAT. The SAT trip was due to water intrusion into the bus duct via a leaking insulator. Degraded caulking and improper design had allowed water to enter between the retaining bolts for the insulator and the bus duct. Loss of the Unit 1 SAT resulted in a loss of the non-essential buses supplied by the SAT. The essential buses were supplied during the entire LOOP from the diesel generators, which automatically started and tied to the buses. Unit 2 was tripped due to loss of non-essential cooling water, which cools many loads including generator auxiliaries, station air compressors, and condensate/condensate booster pumps.

Unit 1 RCS pressure was 350 psig and the temperature was 85ºF. The RCS loops were isolated from the reactor by the loop stop valves to allow draining of the RCS loops to support maintenance. RHR was provided by the 1A RHR pump, which was manually restarted after the diesel generators reenergized the essential AC buses. Byron has the capability to crosstie power between the units to supply essential AC and essential DC power. Byron chose to supply the essential AC buses using the Unit 1 diesel generators instead of supplying them from Unit 2. The diesels supplied power for 29 hours after the LOOP. Byron also did not cross-connect DC power from Unit 2 to Unit 1. DC power remained available via battery chargers, which were powered from the essential buses.

Operation with the RCS loops isolated limits the available methods for cooling the RCS. The cooling methods generally require AC power to be available.

The current ASP models only address LOOP at power; therefore, a separate shutdown event tree model was constructed to represent the conditions that existed during the actual event.

Human Performance Issues

Description	Error Type	Error Subcategory
There was a failure to exchange information between plants owned by the same utility for similar systems. In 1993, the LaSalle station experienced a very similar event caused by water intrusion into a phase duct due to improper maintenance.	Latent	Organizational communication
Maintenance did not properly caulk the channel for the phase duct. Although information from another plant was available, work package development did not incorporate lessons learned.	Latent	Maintenance practices Work practices/Work package development
The design of the weld that runs axially on the top of the channel prevents proper compression of the channel-to-seal duct.	Latent	Design process, failure to identify problems during installation
Inspection was inadequate to identify leakage into the bus ducts or verify the condition of the seals on the bus ducts.	Latent	Testing process Inspection practices

A2.2 Callaway Event, October 17, 1992 (LER 483-92-011)

Synopsis

On October 16, 1992, an annunciator (RK system) field contact power supply failed, causing approximately 76 MCB annunciator windows to be lit. Subsequently, the power supply was replaced and all applicable annunciators cleared.

During restoration from the power supply replacement, all four field contact power supply output fuses blew, causing all RK system MCB annunciators to become inoperable. This resulted in 371 of 683 MCB annunciators becoming lit. Although loss of all RK system annunciators is considered an alert under the plant’s emergency action levels, the licensed operators incorrectly believed that the annunciators remaining dark were operable. The licensed operators were also not aware that all four power supply output fuses had been blown. Therefore, an alert was not declared when required.

Troubleshooting by I&C technicians revealed the four blown field power supply fuses. These fuses were successfully replaced. Other fuses in the logic cabinets of the annunciator system also failed some time during the restoration, but were not initially discovered. Therefore, 164 of the annunciators (those with reflash capabilities) remained inoperable, although the work document was signed off as complete.

During the day shift on October 17, 1992, I&C technicians and the system engineer continued to troubleshoot what was originally believed to be individual annunciator window problems. A logic power supply fuse was replaced, reducing the number of inoperable annunciators to 135. Later, an additional seven fuses in the logic power supplies were replaced. All RK system annunciators were retested and verified operable.

Human Performance Issues

Description	Error Type	Error Subcategory
Plant personnel had inadequate knowledge of how the annunciator system functions during a loss of power.	Latent	Training deficiency
There was no pre-job briefing between the operating crew, the I&C technicians, the planner, and the engineer performing the work. Operations personnel were not informed of the fuses blowing.	Latent	Communications
There was no direct supervision of the I&C technicians during the power supply replacement.	Latent	Management and Supervision
There was an inadequate review and use of the work package because not everyone was familiar with the cautions in the work procedure. There was no documentation of the fuses that were replaced.	Latent	Work package development, QA, and use.
No retest was specified for the field power supply replacement. The testing performed did not reveal that the logic power supply fuses were blown.	Latent	Inadequate post-maintenance testing

A2.3 Calvert Cliffs 2 Event, January 12, 1994 (LER 318-94-001)

Synopsis

On January 12, 1994, Unit 2 tripped when an electrical protective relay actuated in the 13.8 kV voltage regulator for unit service transformer (UST) U-4000-22. This actuation caused the loss of 4 kV buses 22 and 23, and safety bus 24. Both control element drive mechanism motor generator sets lost power, causing a reactor trip from loss of power to the control element drive assemblies and a main turbine trip. Subsequently, similar protective relaying actuated UST U-4000-21, which supplies the redundant Unit 1 4 kV safety bus 14, resulting in a loss of normal power supply to bus 14. At the time of the event, both units were operating at 100% power and a modification was being performed to install six 13.8 kV voltage regulators (three per unit). The project team members incorrectly believed these protective trip circuits were functionally isolated from existing plant equipment. At the time of the event, construction personnel were working on top of the unit 2 voltage regulator 2H2101 and inside each of the three unit 2 voltage regulator transfer switch assembly cabinets. They were preparing 13.8 kV cable ends for termination during future planned 13.8 kV bus outages.

Later, a 13.8 kV feeder breaker to UST U-4000-23 tripped open, resulting in a loss of Unit 2 4 kV buses 25 and 26. This caused the loss of power.

Human Performance Issues

Description	Error Type	Error Subcategory
Control of new equipment under construction was less than adequate. The sudden-pressure-trip circuit was energized and enabled prematurely.	Latent	Work package development, QA and use
The modification process did not adequately require testing to be integrated with work in progress.	Latent	Design change testing
Less than adequate communications existed between project team members. Imprecise terminology was used in project documents and communications.	Latent	Communications
The engineering review of the equipment response during various stages of installation was inadequate.	Latent	Engineering evaluation and review

A2.4 Catawba 1 and 2 Event, February 15, 1993 (LER 413-93-002)

Synopsis

On February 25, 1993, the "B" train Nuclear Service Water (RN) system pump discharge valves failed to open during RN pump start. The discharge valves are designed to automatically open following a pump start. Potential existed that the discharge valves for the "A" train would have a similar problem. Therefore, Technical Specification 3.0.3 was entered for the unit operating at power due to both trains of RN being inoperable. Nuclear Service Water supplies cooling to essential equipment, such as diesel generators and emergency cooling, and non-essential loads. A loss of RN will affect the facilities' capability to respond to a LOCA.

The RN pump discharge valves are motor operated butterfly valves that are interlocked to open when the pump starts and to close when the pump is stopped. The pump starts on a safety injection or loss of offsite power. The valves were failing to open due to incorrect torque switch settings. Due to excessive load on the motor operator, the torque switches were opening prior to the valve being able to open.

Declaring RN inoperable requires declaring both diesel generator operators inoperable. The action statement for both diesel generators being inoperable requires specific surveillance operations to be performed. The surveillance operations were not performed within the required time periods.

Human Performance Issues

Description	Error Type	Error Subcategory
The manufacturer sizing calculations for both the unseating and dynamic torque loads under flow and pressure conditions were incorrect.	Latent	Engineering evaluation and acceptance reviews by facility
There was a lack of detailed information in the motor operated valves (MOVs) torque switch setup procedure.	Latent	Maintenance process, personnel failed to consult additional information sources available
The setting of the torque switches was incorrect.	Latent	Maintenance work package development, QA and use

Description	Error Type	Error Subcategory
The labeling of components in MOVs (torque switches) was inadequate.	Latent	Configuration management/Equipment labeling
Policy guidance for performance of surveillances while in Technical Specification 3.0.3 was not well defined or understood.	Latent	Management policy implementation, lack of knowledge,
Consideration of valve degradation in determining sizing requirements was inadequate.	Latent	Engineering evaluation and review

A2.5 Catawba 2 Event, February 6, 1996 (LER 414-96-001)

Synopsis

On February 6, 1996, while Unit 2 at 100% percent power, ground faults on the resistor bushings for 2A main transformer "X" phase potential transformer and 2B main transformer "Z" phase potential transformer resulted in a phase-to-phase fault. Protective relay actuation on both main transformers resulted in a LOOP. The reactor tripped on reactor coolant pump (RCP) bus under-frequency. As a result of the loss of offsite power, the 2A Emergency Diesel Generator EDG started and sequenced on all required loads. The 2B Emergency Diesel Generator EDG was unavailable due to battery charger repairs; the B train 4 kV essential bus did not automatically reenergize. The cold auxiliary feedwater that was being automatically supplied to the steam generators, in combination with the effects of various steam loads, resulted in a low pressure safety injection. At 1522 hours, the B train 4 kV essential bus was energized from the 2B emergency diesel generator. By 2000 hours, both 4Kv 4 kV essential buses were being supplied from train-related offsite power sources.

The root cause of the event was attributed to the application of the type of resistor bushings used. The use of these resistor bushings in a vertical orientation at the bottom of vertical branch-lines of the isolated phase bus ducting leading to the potential transformers was deficient. The outdoor location and lack of airflow within this portion of the ducting was conducive to moisture intrusion and corrosion. A contributing factor was the lack of adequate preventative maintenance to prevent moisture intrusion/condensation problems.

Human Performance Issues

Description	Error Type	Error Subcategory
The design of bus ducting and resistor bushings failed to minimize moisture intrusion and corrosion in an outside environment.	Latent	Design deficiency
Failure to recognize moisture and corrosion problems.	Latent	Maintenance practices and skill of the craft
There was a lack of adequate preventative maintenance to prevent moisture intrusion/condensation problems.	Latent	Maintenance process and poor work package preparation

A2.6 Fort Calhoun Unit 1 Event, July 3, 1992 (LER 285-92-023)

Synopsis

On July 3, 1992, the licensee returned a non–safety related inverter to service following repairs. When connected to its bus, the inverter output voltage oscillated and caused an electrical supply breaker to electrical panel A1-50 to trip open on high current condition.

Electrical panel A1-50 supplied various instrumentation and components in the plant, including the control circuitry for the main turbine. When power was lost, the circuitry operated as designed and caused the main turbine control valves to close to protect the main turbine.

With the turbine control valves shut, the heat sink for the RCS was temporarily lost, resulting in an RCS pressure increase. The reactor and turbine tripped at approximately 2,400 psia. As pressure continued to increase, the PORVs, the MSSVs, and a pressurizer code safety valve opened to reduce RCS pressure. The PORVs shut at 2,350 psia. The pressurizer code safety valve shut when pressure reached approximately 1,750 psia. RCS pressure increased to approximately 1,925 psia, at which point the pressurizer code safety valve again opened and pressure began to drop rapidly. The operator shut the PORV block valves when the pressurizer quench tank level was observed rising. The pressure drop continued and SI, containment isolation, and ventilation isolation signals were received. All safety systems functioned as designed. The open pressurizer code safety valve partially closed at approximately 1,000 psia and pressure was maintained at that point. An alert was declared.

The cause of the inverter failure was improper maintenance. The safety valve setpoint migrated because the setpoint-locking nut was improperly torqued.

Several positive aspects of staff performance may be seen in the response to this event. Staffing, including use of the shift technical advisor (STA), was adequate. Situational awareness appeared adequate during the event. The crew had previous training on loss of inverter scenarios and the crew reported that the training had helped their ability to respond to these types of events.

Human Performance Issues

Description	Error Type	Error Subcategory
The electro-hydraulic control system (EHC) power supply was changed to non-vital source, but the problem that instigated the change was not corrected by the modification.	Latent (2 errors)	Inadequate design and design change testing for the EHC power supply Inadequate engineering evaluation
The safety valve system design could not tolerate vibrations caused by liquid in the loop seal.	Latent	Inadequate design of safety valve system
The operators' indications did not alert them that the safety valve failed to reseat.	Latent	Ineffective indications to identify an abnormal condition
Previous failures of safety valves were unreported.	Latent	Failure to identify by trending and/or use problem reports
Multiple, previous failures of safety valves were not investigated.	Latent	Failure to respond to industry and internal notices.
After inverter board replacement, there was no method to perform post-maintenance testing without placing the inverter in service.	Latent	Inadequate design and approach to design change testing

Description	Error Type	Error Subcategory
Vendor information was not available and/or requested regarding the correct circuit board configuration.	Latent	Configuration management
Vendor information was not available and/or requested regarding the torque required for the set point locking nut of the SRV after refurbishment.	Latent	Configuration management
The licensee failed to remove a metal jumper and place it on the new board.	Active	Workpackage development, QA and use.
An inverter was placed back into service twice after repairs without full investigation into the cause of failure.	Active	Failure to trend and use problem reports
Operators experienced difficulty in making diagnoses during the event.	Active	Inadequate training and knowledge for degraded computer operations was present.
Known malfunctions existed in computer displays for containment temperature and RCS subcooling.	Latent	Abnormal indications
The licensee failed to establish a fire watch in machinery spaces within 1 hour, per technical specifications.	Active	Operator actions
The licensee failed to respond to fire zone alarm.	Active	Operator actions
An inverter-qualified electrician, who potentially would might have known about the jumpers, was not available.	Latent	Resource allocation.

A2.7 Oconee 3 Event, May 3, 1997 (LER 287-97-003)

Synopsis

On May 3, 1997, Unit 3 was being shut down, with reactor coolant temperature at approximately 240ºF and pressure at 270 psig. A HPI pump and a RCP were in operation. Both letdown storage tank (LDST) level instruments erroneously indicated a constant level of 55.9 in. for about 1 hour, and 45 minutes. During that time, the LDST level actually dropped to the point that damage to the HPI pump resulted.

Complicating Features

Subsequent investigation determined that the common reference leg of the LDST level instruments had been partially drained. Draining the reference leg resulted in the instruments reading high. Incorrect fittings had been used on the reference leg, which allowed it to drain.

Human Performance Issues

Description	Error Type	Error Subcategory
A poor design used a single reference leg for both channels of LDST instrumentation.	Latent	Design deficiency
The licensee had identified the vulnerability as early as 1980 and had proposed solutions, but had not implemented a solution.	Latent	Failure to correct known deficiencies
A precaution did not exist in the shutdown/ cooldown procedure warning of potential common-cause failures of the LDST level instrument.	Latent	Procedures and procedures development
The leaking instrument fitting was due to an inadequate work practice with regard to parts selection.	Latent	Inadequate maintenance work package and practices
Independent observation of control room activities was not being performed. Due to the infrequency and transient nature of shutdown/cooldowns, most power plants assign an independent operator, such as an STA or SRO, to observe.	Active	Command and control and resource allocation
There was a lack of operator sensitivity. The At-The-Controls operator was also the dedicated Low Temperature Over Pressure (LTOP) operator. Too many concurrent duties diverted attention away from monitoring plant parameters. Operators failed to "think ahead" and expect to makeup more often during the cooldown. They did not act on their training and experience. They were relying on the low-level alarm to alert them to the makeup or verify that the makeup had started.	Active	Operator actions
The makeup procedure was deficient. The procedure allowed the LDST level to be maintained in a range lower than the alarm setpoint.	Latent	Procedures and procedures development.
After securing a pump that had started automatically. Operators returned the pump to standby without diagnosing the cause for the auto-start.	Active	Operator actions
Operators failed to diagnose a cavitating pump based on the indications.	Active	Knowledge and training
Operators used an ad hoc, non-systematic approach in responding, which may have contributed to additional HPI pump damage.	Active	Operator action
There were inadequate procedures for failed LDST instrumentation. After the event, operators stated they were unaware that the two level indications shared a common reference leg.	Latent	Training and technical knowledge

Description	Error Type	Error Subcategory
The AIT concluded operations staff had given the impression that the procedures were weak.	Latent	Procedures and procedures development
Operations personnel stated that procedure compliance was not required for events or other operating activities.	Latent	Inadequate knowledge and training regarding conduct of operations
The licensee, in the procedure revision, failed to recognize that there would be no HPI pump discharge pressure indication in the CR control room, due to the required system alignment.	Latent	Procedures and procedures development [Lack of QA and verification during the procedure development process]

A2.8 Oyster Creek Event, May 3, 1992 (LER 219-92-005)

Synopsis

On May 3, 1992, the plant experienced a reactor scram and subsequent Engineered Safety Features systems actuation that were caused by a turbine load rejection. This was due to faults on off-site 230 kV transmission lines caused by a forest fire. The scram occurred at 1326 hours on May 3, 1992, and the event concluded at 0635 hours on May 4, 1992. The reactor was operating at approximately 100% power before the scram. Numerous other engineered safety features actuated including isolation condensers, containment isolation, diesel generator fast start, core spray, and standby gas treatment. Several additional scram signals occurred in the process of bringing the plant to cold shutdown and returning power supplies to off-site sources. An Unusual Event was declared based on high dry well temperature, and an Alert was declared based on the potential of the forest fire to further affect the plant. The plant was brought to cold shutdown at 2234 hours on May 3, and the emergency condition was terminated at 0635 hours on May 4 after off-site power was restored to vital electrical buses. Off-site power had been available since 1331 hours on May 3, but plant management decided not to place the vital buses on off-site power until reliability could be assured. The fire damaged no plant structures or equipment. The forest fire, which caused the loss of off-site power, was the root cause of the event, and the safety significance was minimal because all systems functioned as required.

A loss of power caused a loss of an instrument air. The feedwater regulating valves were locked up and remained in the open position due to the loss of power. When feedwater was restored as required by the EOPs, the operators failed to recognize that the feedwater regulating valves were locked up and failed to close in response to a manual closure signal. Feedwater restoration overfed the reactor, requiring isolation of the isolation condensers to prevent water hammer. Loss of this pressure control method required using the Electro-mechanical Relief Valves (EMRVs) to relieve RCS pressure to the containment. This required use of the Containment Spray System in the torus cooling mode due to the open EMRVs.

An inadequate procedure caused a reactor scram and isolation signal during securing of the diesel generators. Additionally, the operator was monitoring incorrect voltage while securing the diesel generator due to inadequate self-checking and improper labeling.

Human Performance Issues

Description	Error Type	Error Subcategory
The operator failed to recognize the status of Feedwater regulating valves following a loss of air.	Active	Operator action/inaction related to situation awareness
The operating procedure failed to incorporate information already contained in a surveillance procedure for removing a diesel generator from service without causing a scram signal.	Active	Inadequate procedures and procedures development
The operator monitored the incorrect voltage meter.	Active	Knowledge and training

A2.9 Point Beach 1 Event, February 7, 1994 (LER 266-94-002)

Synopsis

On February 7, 1994, with both units operating at full power, EDG G02 was voluntarily removed from service for maintenance. This required placing both units into the LCO defined in Specification 15.3.7.B.1.g, which states that an emergency diesel generator EDG can be inoperable for up to 7 days, provided the other EDG (in this case EDG G01) is tested daily to ensure operability.

The control room received an EDG G01 alarm during a required daily test of EDG G01. A check of the EDG G01 local alarm panel revealed that the fuel pressure alarm was in and the electric fuel oil pump was malfunctioning. EDG G01 continued operating with fuel oil supplied from the shaft driven mechanical fuel oil pump. The mechanical fuel oil pump is fully capable of starting and operating the EDG independently, without reliance on the redundant electric fuel oil pump. Therefore, EDG G01 was operable because the electric fuel pump is not necessary for starting or operating the EDG. EDG G01 was maintained running in an unloaded condition to provide additional assurance that it was operable. The electric fuel oil pump repairs were completed and EDG G01 was shutdown.

EDG G01 was later started and loaded to clean the exhaust system of carbon and other contaminants which that may have built up as a result of running the diesel engine unloaded for an extended period of time during the trouble-shooting and repair of the electric fuel oil pump. Small swings in power on the volt-ampere reactive (VAR) meter were observed. The intensity of these swings increased to the point such that EDG G01 was declared inoperable. Due to Technical Specification requirements for two inoperable diesels, load decreases of 15% per hour were initiated for both units. An Unusual Event was declared based on the loss of both trains of standby emergency power. Engineering and maintenance trouble-shooting determined that the malfunction was caused by shorting of the DC exciter voltage between a rotating bus bar and one of the two stationary brush jumper cables which connects connecting the slip rings within the generator.

The brush jumper cable had been installed in an improper orientation 5 days earlier during the annual maintenance outage on EDG G01. The brush jumper cable was inspected as part of the routine EDG annual maintenance. Based on the inspection, in which some damaged and loose strands were noted near the lug, the brush jumper cable was removed, re-lugged, and replaced. The amount of damaged and loose strands did not pose an operability concern for the EDG; therefore, the re-lugging was not considered absolutely necessary and was performed as normal corrective maintenance.

Human Performance Issues

Description	Error Type	Error Subcategory
Work control for installation of the lug was inadequate.	Latent	Work process; control of unplanned maintenance
Post-maintenance testing failed to inspect for interference while rotating the generator.	Latent	Post-maintenance testing

A2.10 Quad Cities Event, April 22, 1993 (LER 265-93-010)

Synopsis

On April 22, 19993, at 1322 hours, Quad Cities Unit Two was in the shutdown mode at 0% percent of rated core thermal power. At the time, technical staff personnel were performing 4 kV Bus 23-1 Undervoltage Functional Test, QOS 6500-4. During performance of this surveillance, the ½ one-half Diesel Generator Cooling Water Pump (DGCWP) failed to start as required. An Emergency Notification System (ENS) notification was completed at 2145 hours on April 22, 1993.

Human Performance Issues

Description	Error Type	Error Subcategory
An inadequate design prevented operation of the diesel cooling water pump.	Latent	Design process
Some electrical prints were incorrectly or inadequately labeled.	Latent	Configuration management
The electrical drawings do not show the internal breaker logic. This significantly hindered the detection of this design deficiency over the years.	Latent	Configuration management

A2.11 Salem 1 Event, April 7, 1994 (LER 272-94-007)

Synopsis

On April 7, 1994, Unit 1 was operating at a reduced power of 73%. This was due to reduction of condenser cooling efficiency resulting from the river grass (from the Delaware River) that was collecting in the unit's condenser circulating water (CW) intake structure. The CW system traveling screens were becoming clogged, and an increase in condenser backpressure was causing power to decrease. Many of the Unit 1 CW pumps began to trip. The operators attempted to restore the pumps as they tripped, but within 10 minutes of the event, only one CW pump was available. Operators began to reduce plant power in order to take the turbine off line. As a result of equipment complication and operator error, a Unit 1 Reactor trip and automatic safety injection occurred. A subsequent sequence of events resulted in the Unit 1 primary coolant system (PCS) filling, resulting in a loss of normal pressurizer pressure control at normal operating temperature and pressure. The licensee declared an Unusual Event and, subsequently, an Alert Condition at the unit.

During the course of the event, the PORVs actuated over more than 300 times to relieve water and successfully prevent an RCS overpressure condition. One of the primary code safety valves (PR4) was found to have been leaking prior to, during, and following the event, and did not lift during the event.

Performance Insights
During cooldown, use of the Reactor Vessel Level Indication System (RVLIS) is indicated, as there could be possible bubble formation in the vessel. During discussions with operators, however, they stated that they were not required to monitor RVLIS while in cold shutdown, and they generally judged the instrumentation to be incorrect. Training material indicated RVLIS to be correct, and that a fuller understanding of shutdown operations would instill the insight that RVLIS is important to shutdown operations as well.

Human Performance Issues

Description	Error Type	Error Subcategory
Streamlined work controls for handling the river grass intrusion were not adhered to.	Active	Command and Control
Management guidance was lacking for control room operator activities during grass intrusions.	Active	Management Supervision
There was a failure to implement time delays consistent with industry practices when testing solid state logic control for SI.	Latent	Failure to follow industry practices
There was a failure to assign additional operators to the control room when it became known that possible power changes would be necessary with manual rod control.	Active	Resource Allocation
The focus on what was thought to be the primary problem – river grass intrusion – diminished personnel's ability to respond to other problems as they arose.	Active	Operator action/inaction
A rapid downpower with multiple reactivity changes was poorly controlled.	Active	Knowledge and training
Directions from the nuclear shift supervisor (NSS) to the reactor operator for pulling rods to restore Tave were vague.	Active	Command and control
An operator was incorrectly directed to leave reactor console controls when reactivity was not stable.	Active	Command and control
The senior nuclear shift supervisor (SNSS) was outside the control room when needed inside.	Active	Command and control
Continuous and disruptive communications were maintained within the control room.	Active	Communications

Description	Error Type	Error Subcategory
Operators had not been provided direction on action required for operation with reactor temperature below the minimum temperature for critical operations.	Latent	Management and Supervision
Operators failed to anticipate that the cooldown and subsequent heatup would fill the pressurizer.	Active	Knowledge and training
Knowledge of “yellow path” recovery procedures was found to be weak.	Latent	Knowledge and training
Operators forgot or were unaware of reactor power trip on low-power high-flux conditions.	Active	Knowledge and training
For a month prior to the event, the automatic rod control system was not in service, requiring manual mode of operation.	Latent	Failure to correct known deficiencies
Since 1989, it had been noticed that turbine trips produced short-duration high-steam flow signals. However, there was a failure to rigorously analyze this to determine that the cause was from a pressure wave.	Latent	Failure to trend known problems
Automatic controls for the steam generator atmospheric relief valves were not maintained.	Latent	Workpackage, QA, development and use
Operators trained to work around the SG atmospheric relief valve problems.	Latent	Management and supervision endorsement of operator work around
The Licensee previously noted aggravated conditions caused by river grass. A modification was planned but not implemented prior to the event.	Latent	Failure to correct known deficiencies

A2.12 South Texas Project Event, December 29, 1992, to January 22, 1993 (LERs 498-93-005 and 498-93-007)

Synopsis

On January 20, 1993, Unit 1 was operating at 95% power, when EDG 13 failed to start during a monthly surveillance test. The EDG had been painted during a 3-day period beginning December 29, 1992. Paint applied to the fuel injection pump had run into the fuel metering ports, which caused causing the fuel metering rods to bind. An operability test of the EDG had not been performed after the completion of the painting. Following EDG repair, it was returned to service on January 22, 1993, approximately 25 days after it initially had been rendered inoperable. During the time period that EDG 13 was inoperable, EDG 12 had also been removed from service for 61 hours. The TDAFW was also inoperable for the 25-day period that EDG 13 was inoperable.

Human Performance Issues

Diesel Generator DG Inoperability

Description	Error Type	Error Subcategory
No operability testing following external activities.	Latent	Inadequate post maintenance testing
There was inadequate supervision of contract painters to verify that their activities did not affect diesel generator operability.	Latent	Management oversight and inadequate supervision
There was inadequate implementation of lessons learned from industry operating experience concerning diesel generator activities.	Latent	Failure to respond to industry reports
Responsibility for painting was not clearly defined.	Latent	Communications (written and verbal)
The painters failed to adequately ensure that paint did not drip into equipment.	Latent	Inadequate maintenance practices

TDAFW Inoperability

Description	Error Type	Error Subcategory
There was a lack of procedures or manuals and a failure to use best documentation for performing maintenance on safety related equipment.	Latent	Procedures
Safety problem reports were not initiated following previous overspeed conditions.	Latent	Failure to identify by trending reports
Foreign material (i.e., sandblasting compound) was not controlled to prevent contamination and damage to safety-related equipment.	Latent	Inadequate maintenance practices
The failure to maintain consistent testing conditions may have masked turbine degradation. The equipment was not tested under actual standby conditions.	Latent	Inadequate post maintenance testing
Improper configuration of equipment resulted in condensation buildup in steam piping.	Latent	Configuration management/ configuration control
Poorly documented work activities included failing to identify the reason for changes to procedures and anomalies in surveillance results.	Latent	Work package development, QA and use

A2.13 Turkey Point Conditions Since Initial Licensing (1984–1992) (LER 250-92-001)

Synopsis

Since 1984, the plant has routinely placed certain 4160 V volt safety-related breakers in a racked-down configuration. The seismic qualification for the switchgear had been based on all breakers being racked up. On February 10, 1992, the licensee concluded that operability of the switchgear with racked-down breakers (prior to installation of the chocks) could not be assured, and declared the as-found condition to be inoperable and reportable.

Human Performance Issues

Description	Error Type	Error Subcategory
The licensee failed to consider breaker positions when performing seismic analysis.	Latent	Design process
The normal plant condition was not required to meet the parameters of the seismic qualification.	Latent	Procedure and procedures development
Seismic qualification of breakers was not addressed in the licensing basis documents.	Latent	Design process

A2.14 Wolf Creek Generating Station, Docket 50-482 (LER 482-94-013)

Synopsis

On September 17, 1994, with the plant in mode 4 at 300º F and 340 psig, the plant experienced an unanticipated decrease in reactor coolant level due to personnel error. The "A" Residual Heat removal train was lined up to the Reactor Coolant System RCS providing cooldown. The combination of opening two valves resulted in a flow path from the RCS to the reactor water storage tank (RWST). The lineup existed for 66 seconds, during which time 9,200 gallons was drained from the RCS to RWST, causing the RWST to overflowing the RWST. RCS pressure stabilized at 225 psig, which maintained a sub-cooling margin of 90ºF.

Human Performance Issues

Description	Error Type	Error Subcategory
The licensee lacked an understanding of the effect of two simultaneous evolutions.	Latent	Command and control
The licensee inadequately implemented previous industry guidance concerning inadvertent draining of the RCS during RHR operations.	Latent	Failure to respond to industry notices
The licensee failed to have procedural cautions to ensure simultaneous evolution in RHR trains will not result in RCS draining.	Latent	Procedures and procedures development including Preparation of procedural controls
Administrative controls were inadequate to prevent draining the RCS during an evolution with potential for draining.	Latent	Procedures and procedures development

Description	Error Type	Error Subcategory
Shift Supervision failed to inform the crew of on-going evolutions.	Active	Command and control

APPENDIX B

ACTIVE AND LATENT FAILURES FOR SPECIFIC EVENTS

B1. Human Performance Errors Analyzed by Event

Table B-1 presents human error category and subcategory information. This information is presented on an event-by-event basis for each event analyzed in the present study. "A" stands for active errors, and "L" stands for latent errors. The categories and subcategories are the same as those used in Table 3-2. Six major categories are covered: operations; design and design change work practices; maintenance practices and maintenance work control; procedural design and development process; corrective action program; and, management oversight. Each of these categories has a number of subcategories. The 21 subcategories are read as columns at the top of the table. For example, the "Operations" category consists of command and control including resource allocation; inadequate operator knowledge or training; incorrect operator actions and or inactions; and communication failures. Thirty-seven events are qualitatively analyzed; the first twenty-three were also subject to SPAR analysis.

Table B-1. Active and Latent Errors for Specific Events.

	Command and Control Including Resource Allocation	Inadequate Knowledge or Training (Ops)	Incorrect Operator Action/Inaction	Communications	Design Deficiencies	Design Change Testing	Inadequate Engineering Evaluation/Review	Ineffective Abnormal Condition Indication	Configuration Management	Work Package Development, QA & Use	Inadequate Maintenance & Maintenance Practices	Inadequate Technical Knowledge (Maint.)	Inadequate Post-Maintenance Testing	Inadequate Procedures/Procedure Development	Failure to Respond to Industry & Internal Notices	Failure to Follow Industry Practices	Failure to Identify by Trending & Use Problem Reports	Failure to Correct Known Deficiencies	Inadequate Supervision	Inadequate Knowledge of Systems & Plant Operations	Organizational Structure	
Facility/LER	Operations				Design and Design Change Work Practices					Maintenance Practices and Maintenance Work Control					Corrective Action Program and Learning				Management and Supervision			TOTAL
ANO 1 31396005					L(2)	L									L		L	L(2)	L			8
ANO 2 36895001					L	L	L															3
Beaver Valley 1 33493013	L				L						A											3
Comanche Peak 44595003/004					L(3)					L	L(2)											6
D.C. Cook 31595011												L		L								2
Dresden 3 24996004		L									L(2)					L	L	L				6
Haddam Neck 21993006/007		L(2)	L(2)				L(5)		L(2)		L(2)											13
Hatch 1&2 37200002	A	AL	A		L									L	L							7
Indian Point 2 24799015 AIT 50-247-99-08	A(3)	AL		L(2) A(2)		L	L		L(3)		L			L(3)			L	L(2)		L		22
LaSalle 1 37393015					L						L(5)			L				L				8

Facility/LER	Command and Control Including Resource Allocation	Inadequate Knowledge or Training (Ops)	Incorrect Operator Action/Inaction	Communications	Design Deficiencies	Design Change Testing	Inadequate Engineering Evaluation/Review	Ineffective Abnormal Condition Indication	Configuration Management	Work Package Development, QA & Use	Inadequate Maintenance & Maintenance Practices	Inadequate Technical Knowledge (Maint.)	Inadequate Post-Maintenance Testing	Inadequate Procedures/Procedure Development	Failure to Respond to Industry & Internal Notices	Failure to Follow Industry Practices	Failure to Identify by Trending & Use Problem Reports	Failure to Correct Known Deficiencies	Inadequate Supervision	Inadequate Knowledge of Systems & Plant Operations	Organizational Structure	TOTAL
	Operations				Design and Design Change Work Practices					Maintenance Practices and Maintenance Work Control					Corrective Action Program and Learning				Management and Supervision			
Limerick 1 35295008											L	L							L			3
McGuire 2 37093008	AL	AL	A(2)		L				L				L(2)			L		L(2)				13
Millstone 2 33695002							L												L			2
Oconee 1,2,&3 26992018					L	L	L			L	A											5
Oconee 2 27097001							L(2)				L				L	L		L	L			7
Oconee 2 27092004	A	L		A(2)	L(2)			A		L(2)	A			L(6)	L		L		L			19
Perry 1 44093011											L(2)	L							L			4
Riverbend 45894023		L		L			L		L	L	L(2)											7
H.B. Robinson 26192017/013/018					L						L(2)	L										4
Seabrook 44396003					L					L					L		L					4

Facility/LER	Command and Control Including Resource Allocation	Inadequate Knowledge or Training (Ops)	Incorrect Operator Action/Inaction	Communications	Design Deficiencies	Design Change Testing	Inadequate Engineering Evaluation/Review	Ineffective Abnormal Condition Indication	Configuration Management	Work Package Development, QA & Use	Inadequate Maintenance & Maintenance Practices	Inadequate Technical Knowledge (Maint.)	Inadequate Post-Maintenance Testing	Inadequate Procedures/Procedure Development	Failure to Respond to Industry & Internal Notices	Failure to Follow Industry Practices	Failure to Identify by Trending & Use Problem Reports	Failure to Correct Known Deficiencies	Inadequate Supervision	Inadequate Knowledge of Systems & Plant Operations	Organizational Structure	TOTAL
Facility/LER	Operations				Design and Design Change Work Practices					Maintenance Practices and Maintenance Work Control					Corrective Action Program and Learning				Management and Supervision			TOTAL
Sequoyah 1&2 32792027	A	A	A(2)	L					L	L(2)			L	L								10
St. Lucie 1 33597011				L		L(2)	L		L					L							L	7
Wolf Creek Generating Station 48296001	A	L	A(2)	A	L		AL				L			L								10
Byron 45496007					L					L	L				L							4
Calloway 48392011		L		L(2)		L				L									L			6
Calvert Cliffs 31894001				L		L	L			L												4
Catawba 41393002		L					L(2)		L		L			L								6
Catawba 41396001					L					L	L											3
Fort Calhoun 28592023		L	A(2)		L(2)	L	L	AL	L(2)	AL		L					L(2)					16
Oconee 3 28797003	A	AL	A(3)		L						L			L(5)				L				14

	Command and Control Including Resource Allocation	Inadequate Knowledge or Training (Ops)	Incorrect Operator Action/Inaction	Communications	Design Deficiencies	Design Change Testing	Inadequate Engineering Evaluation/Review	Ineffective Abnormal Condition Indication	Configuration Management	Work Package Development, QA & Use	Inadequate Maintenance & Maintenance Practices	Inadequate Technical Knowledge (Maint.)	Inadequate Post-Maintenance Testing	Inadequate Procedures/Procedure Development	Failure to Respond to Industry & Internal Notices	Failure to Follow Industry Practices	Failure to Identify by Trending & Use Problem Reports	Failure to Correct Known Deficiencies	Inadequate Supervision	Inadequate Knowledge of Systems & Plant Operations	Organizational Structure	
Facility/LER	Operations				Design and Design Change Work Practices					Maintenance Practices and Maintenance Work Control					Corrective Action Program and Learning				Management and Supervision			TOTAL
Oyster Creek 21992005		A(2)												A								3
Point Beach 1 36694002										L			L									2
Quad Cities 2 26593010					L				L(2)													3
Salem 1 27294007	A(5)	A(2) L	AL	A							L					L	L	L(2)	A			17
South Texas 1 49893005/007				L					L	L	L(2)		L(2)	L	L		L		L			11
Turkey Point 25092001					L(2)									L								3
Wolf Creek Generating Station 48294013	AL													L(2)	L							5
Number of Events	10	15	8	10	18	8	12	2	10	13	20	5	4	14	8	4	8	8	9	1	1	
Percentage of Events	27.0	40.5	21.6	27.0	48.6	21.6	32.4	5.4	27.0	35.1	54.1	13.5	10.8	37.8	24.3	11.0	21.6	21.6	24.3	2.7	2.7	
Total Errors	18	23	16	15	24	9	19	3	15	16	31	5	6	26	8	4	9	12	9	1	1	

APPENDIX C

ANALYSIS OF HUMAN ERROR TO PRA BASIC EVENTS

Table C-1. Analysis of Human Error to PRA Basic Events

EVENT	PRA BASIC EVENTS	HUMAN ERROR	COMMENTS
Wolf Creek Generating Station, January 30, 1996 LER 482-96-001	IE-TRAN, AFW-MDP-CF-AB, AFW-MDP-FC-1A, CVC-MDP-CF-RUN, CVC-MDP-FC-1A, EPS-DGN-CF-ALL, EPS-DGN-FC-1A, HPI-MDP-CF-ALL, HPI-MDP-FC-1A, MFW-XHE-NOREC, RHR-HTC-CF-ALL, RHR-MDP-CF-ALL, RHR-MDP-FC-1A, Transient initiating event, train A of ECCS systems and common cause failure of all ECCS systems.	The incorrect lineup of the ESWS was not corrected after it was identified.	Frazil icing build-up on the Circulating Water System traveling screens caused a reactor trip and loss of cooling water to the A train of ECCS systems, with the potential to cause loss of all ECCS trains.
		An unfamiliar evolution for ESWS was performed without using a procedure or having a second operator verify the lineup using the procedure.	
		Knowledge and training for conditions that will cause Frazil icing and the effects of Frazil icing were inadequate.	
		Design of warming lines was inadequate.	
		Procedures to identify and respond to Frazil icing of the trash racks were lacking.	
		A technical specification interpretation previously had indicated, incorrectly, that Frazil icing conditions could not occur in the ESW pump house due to its being enclosed and heated.	
		Information transfer concerning the status of the ultimate heat sink was inadequate.	

EVENT	PRA BASIC EVENTS	HUMAN ERROR	COMMENTS
Wolf Creek Generating Station, January 30, 1996 LER 482-96-001 (continued)	AFW-TDP-FC-1C, turbine-driven AFW pump train failure	None.	Packing leakage caused pump to be declared inoperable.
Oconee 2, October 19, 1992 LER 270-92-004	IE-LOOP	Work package lineup placed battery charger in a line up without the battery connected, which is outside the design capabilities of the battery charger.	Problems with manipulations associated with the battery charger and bus transfers were the cause of the LOOP.
		The AIT team concluded that the live bus transfer procedure and training were not adequate.	
		The battery charger was not fully sized to replace the battery in the configuration as placed.	
	EPS-HEU-CF-KEOWE, common cause failure of both Keowee hydro units.	Accident analysis planning did not fully envelop the extent of Keowee hydroelectric station's critical role in terms of mitigation and recovery.	
		Procedures were not fully developed to support handling of the event; Keowee operators had no specific procedure for responding to or verifying emergency start of the Keowee hydro units.	
		Keowee operators demonstrated lack of knowledge of how to respond to their control room annunciation of abnormal conditions.	

EVENT	PRA BASIC EVENTS	HUMAN ERROR	COMMENTS
Oconee 2, October 19, 1992 LER 270-92-004 (continued)	EPS-HEU-CF-KEOWE, common cause failure of both Keowee hydro units. (continued)	Oconee Unit 2 procedures did not require verification of the proper operation of the Keowee hydro generators either from available Oconee indications or from the on-shift Keowee operators.	
		Oconee CR personnel and management were not aware of the “de-energized /overheat-feeder-interlock” feature. (Unit 2 trips when Unit 1 is shutdown because no voltage is present on the overhead path.) This resulted in an inadvertent loss of both Keowee units during the recovery phase.	
		The level and significance of problems at Keowee during the event were not fully communicated nor understood.	
		Keowee annunciator and computer alarm printers were lost when auxiliary buses supplying power to them failed.	
		An MG-6 relay at Keowee failed due to excessive resistance; a similar problem had been identified in September 1992.	
		Keowee took actions without concurrence or direction from Oconee control room even through it had an impact on the Oconee emergency power.	
		Nonexistent Keowee emergency procedures for this and other similar sequences.	

EVENT	PRA BASIC EVENTS	HUMAN ERROR	COMMENTS
Oconee 2, October 19, 1992 LER 270-92-004 (continued)	EPS-BAC-LF-MFB1, EPS-BAC-LF-MFB2, Failure of main feeder buses 1 & 2.	No guidance existed in procedures for recovery from an improper lineup.	
		Complex and atypical design including the emergency power system, and interacting systems contributed to problems while operating these systems.	
Perry, April 19, 1993 LER 440-93-011	RHR-STR-CF-SPOOL, common cause failure of suppression pool strainers.	Inadequate inspection processes failed to identify a problem during previous inspections.	Failure of all suppression pool strainers leads to failure of all ECCS.
		Material control during maintenance activities performed in the containment was inadequate.	
		Management failed to set cleanliness expectations for the containment and suppression pool.	
		Personnel sensitivity to effects of cleanliness on ECCS operability was inadequate.	
Oconee 2, April 21, 1997 LER 270-97-001	IE-SLOCA, small loss-of-coolant accident initiating event, HPI-MOV-CC-DISA, failure of HPI cold leg injection path A.	An effective HPI nozzle inspection program based on available industry recommendations was not implemented.	A small LOCA was assumed for the PRA event assessment. Basic event HPI-MOV-CC-DISA represents failure of the HPI cold leg injection path, including the nozzle.
		There was a failure to effectively address known problems and implement appropriate corrective actions.	
		There was inadequate consideration of the effect of thermal stress on nozzles.	

EVENT	PRA BASIC EVENTS	HUMAN ERROR	COMMENTS
Oconee 2, April 21, 1997 LER 270-97-001 (continued)	IE-SLOCA, small loss-of-coolant accident initiating event, HPI-MOV-CC-DISA, failure of HPI cold leg injection path A. (continued)	Plant operations were not managed to minimize thermal stresses.	A small LOCA was assumed for the PRA event assessment. Basic event HPI-MOV-CC-DISA represents failure of the HPI cold leg injection path, including the nozzle (continued).
		UT testing as scoped was not thorough enough to identifying these problems.	
		Evaluation and interpretation of RT test findings was inadequate.	
Limerick 1, September 11, 1995, LER 352-95-008	IE-TRAN, Transient Initiating Event. PPR-SRV-00-1VLV, Main Steam Safety Relief Valve.	Engineering review of previous test results on the SRV was inadequate.	Failure to recognize previous seat leakage as coming from pilot valve and not the main valve allowed SRV to open.
	RHR-STR-CF-SPOOL, common cause failure of suppression pool strainers.	Material control during maintenance activities performed in the containment was inadequate.	Approximately 1400 pounds of debris was removed from the suppression pool after this event.
		Management failed to set cleanliness expectations for the containment and suppression pool.	
		Personnel were not sufficiently sensitive to effects of cleanliness on ECCS operability.	

EVENT	PRA BASIC EVENTS	HUMAN ERROR	COMMENTS
Indian Point 2, August 31, 1999 LER 247-99-015 AIT 50-247/99-08	IE-LOOP, Loss of Off-site Power Initiating Event.	The station auxiliary transformer load tap changer was not maintained in the automatic position as required by the licensing bases.	Modeled as a LOOP initiating event.
		The degraded voltage relay reset values for the 480 V buses were not controlled.	
		Station personnel missed an earlier opportunity to identify the Amptector test methodology problem.	
		Corrective actions for previous breaker problems, which addressed test methodology, were overdue and incomplete.	
		Station personnel did not evaluate the station auxiliary transformer load tap changer condition report for safety and operability impact.	
		Procedures had not been implemented to reflect the required operational mode of the load tap changer for compliance with plant design basis.	
	EPS-DGN-FC-23, failure of EDG 23	The 23 EDG output breaker over-current setpoint was not properly controlled due to an inadequate test methodology.	PRA cascaded this failure to vital bus 6A and its safety-related loads (one AFW train and one PORV block valve).
		The 23 EDG output breaker over-current setpoint was not properly controlled due to an inadequate test methodology.	
		The 23 EDG load sequencing had been changed and, within relay tolerances, allowed multiple pump motors to load onto the bus at one time.	

EVENT	PRA BASIC EVENTS	HUMAN ERROR	COMMENTS
Indian Point 2, August 31, 1999 LER 247-99-015 AIT 50-247/99-08 (continued)	Not Applicable.	Engineering personnel did not investigate the cause of an OT?T signal increase that had occurred on August 26, 1999.	These human errors contributed to the initial upset condition of the reactor trip, triggering the LOOP. Had other failures not been present to cause the over-riding LOOP, this event would have been modeled as a reactor trip.
		Station personnel failed to recognize and evaluate a potential trend in RPS problems and failures.	
		Work control personnel were not notified of the spurious trips in the OT?T circuitry for consideration in work planning.	
Hatch, January 26, 2000 LER 321-00-002	IE-TRAN, Transient Initiating event.	Industry notices for GE Control switches used to position inlet valves were not implemented.	Contributed to partial loss of feedwater initiating event.
	OPR-XHE-XE-HPINJ, operator fails to control high pressure injection sources, TRANS-XX-NR, transient sequence XX recovery factors.	Operators failed to observe automatic flow demand before transferring HPCI control from manual back to automatic.	Recovery of HPCI and RCIC are part of the sequence recovery factors.
		RCIC restart procedures were inadequate.	
		RCIC restart training was inadequate.	

EVENT	PRA BASIC EVENTS	HUMAN ERROR	COMMENTS
McGuire 2, December 27, 1993, LER 370-93-008	IE-LOOP, LOOP initiating event.	Licensee did not appear to understand the switchyard relay protection scheme, therefore allowing a design to exist that placed undue reliance on a non-safety related turbine runback feature to function correctly.	Failure of the turbine-generator to runback in combination with a bus line insulator failure caused the second bus line to trip, resulting in a LOOP.
		There was no testing program for the turbine runback feature, which might have identified the potential design and configuration problems.	
	IE-SGTR, SGTR initiating event. MSS-VCF-HW-ISOL, failure to isolate a ruptured SG.	Maintenance and testing procedures for the MSIVs failed to incorporate vendor recommendations.	Given the steam generator differential pressure and conditions during the event (caused by the MSIV leakage), the ASP analysis increased the SGTR initiating event frequency by four orders of magnitude. The MSIV failure would also prevent isolation of a ruptured steam generator.
		There was no post-modification testing on the MSIV after a modification removed additional closing force from air pressure. There was a failure to detect a significant change in the valve's performance.	
		Excessive time was taken to read the EOP foldout pages, delaying the implementation of procedural steps to isolate MSIVs prior to a SI signal.	

EVENT	PRA BASIC EVENTS	HUMAN ERROR	COMMENTS
McGuire 2, December 27, 1993, LER 370-93-008 (continued)	IE-SGTR, SGTR initiating event. MSS-VCF-HW-ISOL, failure to isolate a ruptured SG. (continued)	Instrumentation and electrical personnel took actions, on their own initiative, without procedural direction and without use of reference material (i.e., CR drawings) that opened the MSIV upstream drain lines that were isolated.	Given the steam generator differential pressure and conditions during the event (caused by the MSIV leakage), the ASP analysis increased the SGTR initiating event frequency by four orders of magnitude. The MSIV failure would also prevent isolation of a ruptured steam generator. (continued)
		Operators did not recall that the drain valves had been modified, changing their fail-safe position from open to closed on loss of power. Operators relied on past experience and simulator training rather than training that emphasized the modifications.	
	PPR-SRV-CO-L PPR-SRV-CO-SBO PPR-MOV-FC-BLK1 PPR-MOV-CC-BLK1 PPR-SRV-CC-PRV1	None.	PORV C was out of service for a plant modification at the time of the event.

EVENT	PRA BASIC EVENTS	HUMAN ERROR	COMMENTS
Robinson 2, July – August, 1992 LER 261-92-013, -014, &-017	IE-LOOP, LOOP initiating event.	Improper operation and/or maintenance caused the junction box to be rotated to a position that did not allow for proper drainage.	Water accumulation in the junction box shorted a relay in the sudden pressure fault protection relay sensing circuitry. This caused the start-up transformer to trip and ultimately a LOOP.
		The junction box was improperly designed in that it did not include necessary fasteners to assure that it remained in an orientation that allowed for drainage.	
	HPI-MDP-FC-2A, HPI-MDP-FC-2B, HPI-MDP-FC-2C, failure of safety injection pump trains A, B, & C.	Debris from failed dams was not removed. Concern and action for debris in system connection to the RCS were inadequate.	Safety Injection pump trains A and B were declared inoperable and modeled as failed. The failure probability for Pump Train C was doubled to model the potential increase in failure by this common cause mechanism.
		QA was inadequate to ensure maintenance of system cleanliness.	
Haddam Neck, May-June, 1993 LER 213-93-006 LER 213-93-007 AIT 213/93-80	MCC-BUS, failure of MCC-5.	The manufacturer of the breakers failed to incorporate information in vendor manuals even though information was incorporated in another breaker manual that used identical relays.	Resulted in undetected failure of MCC-5 during LOOP for a long duration.
		There was a failure to determine a positive root cause for previous failures of the same relay.	
	PPR-SRV-CC-PRV1, failure of PORV.	An improper valve lineup prevented monitoring moisture content in the air system, which would have allowed for early detection and correction of the problem.	PORV failure rate was increased by a factor of 27 to 0.17 based on this error.

APPENDIX D

REVIEW OF IPE (NUREG 1560) COMPARATIVE REVIEW OF RELATED HUMAN PERFORMANCE ANALYSES

D1. NUREG-1560 Overview

NUREG-1560, *Individual Plant Examination Program Perspectives on Reactor Safety and Plant Performance* contains a summary analysis and review of licensee PRA & HRA submittals. Note that the IPE submittals generally were summaries of the analyses and did not provide as much detail in the documentation as would be expected of a full PRA. To fully appreciate the HRA analyses performed in conjunction with the IPEs, interviews with the appropriate HRA analysts would be needed. Such an effort was not within the resources of this project.

The HRA portions of the NUREG were reviewed to gain insights regarding the characterization of human performance in events including identification of risk-significant human errors. A number of conclusions could be drawn. First, the licensees did not appear to use operating events as a technical basis for HRA performed in their IPEs. Second, there was considerable variability in the HRA methods used. Third, the IPEs focused on post-initiator activities on the part of operators and crews. Therefore, with only minor exceptions (i.e., some studies did acknowledge the contribution of calibration errors to plant risk), they did not dwell upon the role of the types of latent errors determined to be important in the present study..

D1.1 NUREG-1560 Performance Insights

NUREG-1560, *Individual Plant Examination Program Perspectives on Reactor Safety and Plant Performance,* documents the results of the effort by the Office of Nuclear Regulatory Research to identify significant safety insights based on IPEs for the different reactor and containment plant designs. The major objectives of that program were to provide perspectives on: (a) the impact of the IPE program on reactor safety; (b) plant-specific features and assumptions that play a significant role in the estimation of CDF and the analysis of containment performance; (c) the importance of the operator's role in CDF estimation and containment performance analysis; and, (d) evaluate the IPEs with respect to risk-informed regulation.

The INEEL reviewed the results of NUREG-1560 to determine the role of human performance and identify the ways in which human performance has been associated with risk. This section documents the results of that review.

D1.2 Summary and Overview of IPEs

A quality Level 1 PRA comprises the following elements:

- Delineation of event sequences that, if not prevented, could result in core damage and the potential release of radio nuclides
- Development of models that represent core damage sequences
- Quantification of the models in the estimation of the core damage frequency.

Human error identification and quantification are important parts of a quality PRA. HRA involves evaluating the human actions that are important in preventing (or causing) core damage. HRA requires skills in human factors, including cognition, systems, risk, and procedure implementation and practices, to determine the types and likelihood of human errors germane to the sequence of events that could result in core damage.

For a PRA to be complete, it must identify operator actions important to preventing core damage. In the IPE submittals, nearly all of the important human actions involve the failure to respond to a degraded condition of certain systems or components and overcome the failure and achieve a desired result. The actions that are important at plants appear in many cases to depend on plant-specific design features (i.e., stabilization). It also appears to depend on differences in the analyses themselves, (i.e., the process and results of identifying important human actions). Some of the plant-specific differences are as follows:

- Defense in depth and availability of alternate paths to achieve success
- Automation of certain functions
- Time constants of plants and the resulting time available for successful operator action
- Configuration of electrical systems and logic that do/do not trigger systems
- Whether credit is given for an operator action (i.e., some plants do not model operator actions as a potential recovery mechanism for certain systems, or simply assume failure).

Considerable variability has been found in the PRA treatment of the kinds of actions that are important in plants. In BWRs, only four classes of human actions were found to be important across plants. In PWRs, three classes of human actions were found to be important across plants. Pre-initiator actions that are important in PRAs were common in less than 25% of the plants, across both BWRs and PWRs. These relate to miscalibration or failure to restore systems after testing or maintenance. For the most part, the human contributions to core damage frequency range between from 1 to 10%. A few exceptions are noted outside this range.

HRA methods are biased to the types of human performance they identify. The human reliability techniques used in the IPEs typically treat human error as a random event that is affected by the type of task and the intrinsic and extrinsic factors that may impinge upon the operator or crew at the time of performance. There are limitations to such approaches both for the identification and quantification of human error and reliability. That the methodology itself can influence the failure rates produced may be problematic for several reasons. First, true variability ought to be due only to plant-, initiator-, and sequence-specific factors or to factors that are intrinsic to the task. To the extent that the method contributes to the variability, it is undesirable. Second, such variability may contribute to overly pessimistic or optimistic estimations of the failure likelihood. Assumptions that are driven by the method that produce such results will result in either over-compensation for the error, (e.g., by training, procedures, human-machine interface (HMI) modifications, etc.) or under-compensation (e.g., inadequate controls to prevent or mitigate them). In either case, such variability may result in a licensee perception of the likelihood of the failure and its significance that may be wrong.

As the authors of NUREG-1560 discuss, reasonable explanations for variability in the HEPs produced by different plants do not necessarily imply that the HEP values are generally valid. Nor should the discussion of variability bear upon the issue of validity. Consistency can be obtained through HRA without necessarily producing valid HEPs. It is currently the situation with these and other HRA methods, that processes and metrics for their validation have not been produced. Hence, validation of results from IPE submittals, as well as for other applications of HRA, is not currently forthcoming.

D1.3 Scope of the IPE Human Action Review

The Human Reliability Analysis of each IPE formed the basis of the reviews in NUREG-1560. HRAs document operator actions and error probabilities and may also address assumptions used in modeling human actions, uncertainties, source documents, subject matter experts interviewed, and other information considered relevant by analysts in documenting their estimation of human failure likelihood. The INEEL staff reviewed the insights. Two primary issues were the focus of the current review:

- Identifying operator actions critical to preventing core damage
- Consistency and reasonableness in the approach and results of quantifying human failure.

The first issue addresses the completeness of analyses; the second addresses reliability of processes and methods. Both affect how and whether the human contribution to reactor safety is identified and adequately addressed in the industry.

D1.4 Critical Operator Actions

D1.4.1 Boiling Water Reactors

Few specific human actions are regularly found to be risk-important across all BWR IPEs. Twenty-seven BWR submittals form the sample used to analyze human actions. Only four human actions were found to be common in 50% (~14) or more of the IPEs. These actions are post-initiator and include the following:

- Perform manual depressurization
- Vent containment
- Align containment or cool suppression pool
- Initiate standby liquid control.

Two actions were found to be important in 25% (~8) of the submittals:

- Adjust level control in anticipated transient without scram
- Align/initiate alternative injection.

In the case of manual depressurization, the percentage of total CDF accounted for by cutsets, including this event, ranged from 1 to 44%. In the case of decay heat removal, the contribution of human failures to these events ranged from 1 to 5% in resulting CDF. CDF contributions from aligning and initiating alternate injection sources range from 1 to 4%.

Pre-initiator human actions were found to be important for some licensees. The majority of these relate to calibration errors or failures to restore systems to service. Such failures have been termed latent because they produce a failed component or system that awaits demand or use for its effect(s) to be produced. Such human actions were found in ~20% of licensee submittals. Some licensees may not have considered such pre-initiator events.

Further analyses were documented in NUREG-1560 to attempt to relate important human actions to major classes of BWRs (e.g., BWR1). While several instances were identified in which a human action could be related to a class of BWR, most of the differences in identifying important human actions across BWR classes seemed to have more to do with modeling of human actions or plant-specific differences.

D1.4.2 Pressurized Water Reactors

Just three human actions, or human action sequences, were found to be important in more than 50% of PWR submittals. PWR submittals cover three different vendors and five discernible plant types (i.e., Babcock & Wilcox, Combustion Engineering (CE), and Westinghouse 2-, 3-, and 4 -loop plants).

The important human actions are:

- Switchover to recirculation (i.e., plants with manual or semiautomatic switchover)
- Feed and bleed cooling
- Depressurization and cool down.

For human actions relating to switchover to recirculation cooling, plant-specific differences are important. All of the CE plants have automatic switchover, as do four of the other plants. Of the remaining plants, 80% found this action to be important. Those that did not may have different refueling water storage tank capacities, thereby lessening the importance of the recirculation function. The contribution from this failure to CDF ranges from less than 1 too as much as 16%, with an average of 6% contribution. Plant-specific differences, most notably the reliability of plant AFW and EFW, affect the relative importance of feed and bleed cooling in PRAs. For those that find feed and bleed cooling to be important, the CDF contribution from this event ranges from less than 1 to 11%, with an average contribution of 4%. Human actions relating to depressurization and cool down are estimated to have similar contributions to CDF in those event sequences where these actions are important, ranging from less than 1 to 7%, with an average of 4% contribution to CDF.

Pre-initiator events, including miscalibration and restoration failures, were important as defined by Fussel-Vesely importance measures and were present in approximately 25% of submittals. For example, failures in calibrating pressure, level, and temperature sensors and transmitters were identified in PWR submittals. Licensees also identified human actions that produced restoration failures.

The authors of NUREG-1560 observe that neither BWR nor PWR submittals show a broad consistency in terms of which human actions are found to be important. Furthermore, in both BWRs and PWRs, no individual human action appears to account for a large percentage of the total CDF across submittals. However, human actions are important contributors to operational safety.

D1.5 Error Quantification in IPEs

A number of HRA methods were used in the IPEs. These can be grouped into the following categories:

- A Technique for Human Error Rate Prediction (THERP) and THERP derivatives;
- Performance-shaping factor methods
- Time-reliability methods
- Hybrid combinations.

Three factors were deemed to affect the quantification or application of the HRA methods:

- The extent to which accident progression and performance shaping factor (PSF) effects were taken into account
- Whether simulator exercises were used, and
- Whether analysts conducted walkdowns.

Further analyses were performed to study the variability in HEPs produced by different methods. In principle, variability may not be a concern if valid reasons underlie the results. Furthermore, reliability or consistency in results may not be of highest priority for PRAs if validity is sacrificed. Assuming there are valid reasons for variation; however, reliability and consistency in results should be produced.

The NUREG-1560 review of BWR actions showed that depressurization failure estimates were included in 26 BWR PRAs. Significant variability was found in the resulting HEPs. HEPs ranged from ~1 E-5 to 3 E-1. A variety of apparently valid reasons are cited for such variation:

- Depressurizing by nonstandard means
- Recovery of a failed automatic depressurization, complicated by secondary failures
- Number of SRVs available
- In-sequence human failure dependencies
- Initiator- and sequence-specific factors.

NUREG-1560 cites the following reasons for HEP variability:

The HRA methodology used

- The way the HRA methodology was applied
- Optimistic or pessimistic assessments of task-specific features that would affect operator reliability.

NRC FORM 335 (2-89)