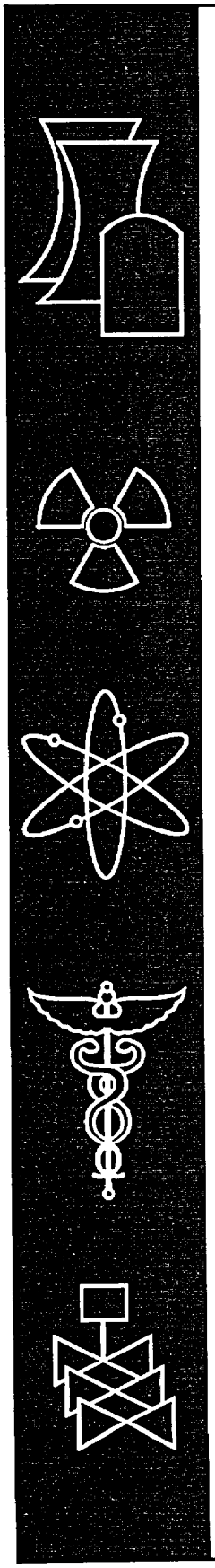
NUREG/CR-6775
INEEL/EXT-01-01167



Human Performance Characterization in the Reactor Oversight Process

Idaho National Engineering and Environmental Laboratory

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

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: Office of the Chief Information Officer,
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

NUREG/CR-6775
INEEL/EXT-01-01167

Human Performance Characterization in the Reactor Oversight Process

Manuscript Completed: September 2001
Date Published: September 2002

Prepared by
D. I. Gertman, B. P. Hallbert, D. A. Prawdzik

Idaho National Engineering and Environmental Laboratory
P.O. Box 1625
Idaho Falls, ID 83415-3129

E. A. Trager, NRC Project Manager
J. Kramer, NRC Technical Monitor

Prepared for
Division of Systems Analysis and Regulatory Effectiveness
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC Job Code E8238

ABSTRACT

A review of the Reactor Oversight Process (ROP) and its characterization of human performance was performed by the Idaho National Engineering and Environmental Laboratory (INEEL) to describe the means by which the Nuclear Regulatory Commission (NRC) monitors, analyzes and feeds back information on human performance. Review of detailed human performance findings and trends observed in 37 operating events identified through the Accident Sequence Precursor (ASP) program served as the sample of operating experience. All events reviewed had a conditional core damage probability of 1.0E-5 or greater and indicated the influence of human performance. Reviews also considered Individual Plant Examinations (IPEs) and Augmented Inspection Team (AIT) reports. These reviews were then compared to ROP source materials. The ROP source materials included SECY-99-007/007A, SECY-00-0049, NRC manual chapters and inspection procedures, inspection and supplementary inspection reports, plant issues matrices (PIMs) risk-informed inspection notebooks, and the Significance Determination Process (SDP) for Operator Requalification. Insights regarding the characterization of human performance in the ROP are presented.

Contents

LIST OF TABLES

LIST OF APPENDICES

EXECUTIVE SUMMARY

Understanding that human performance and error contributes to the root causes that underlie performance problems in nuclear power plants, the US Nuclear Regulator Commission (NRC) established human performance as a crosscutting issue as part of their Reactor Oversight Process (ROP). This was confirmed and is characterized by research on the risk impact of human performance in operating events (NUREG/CR-6753, 2001). Work being summarized here documents how the ROP monitors, analyzes, and feeds back information on human performance and compares it to findings from the review of operating events. In general, the ROP is likely to capture important issues through a combination of baseline inspections, supplemental inspections, performance indicators, cornerstones, and cross-cutting issues. The ROP documents performance issues through operator requalification inspections, the significance determination process, inspector observations documented in inspection reports as "no color findings," trended issues, or from reviews of licensee corrective action programs. Recurrent problems at plants, identified through review of events underscore the importance of problem identification and resolution as part of the regular baseline inspection process. An Idaho National Engineering and Environmental Laboratory (INEEL) review of inspection report findings indicated that latent error conditions were reported three times more frequently than active errors. This trend is in the same general direction as the ratio of 4:1 latent to active errors obtained in previous studies. (NUREG/CR-6753, 2001)

Findings

The working hypothesis for this effort was that the ROP identifies the same human performance issues that were identified through analyses of operating events. This project found this to be the case; the ROP has the potential to identify the same human performance issues contributing to significant operating events. Many of these issues are likely to be contained in "no color findings" in baseline inspection reports, in plant issues matrices (PIMs), in problem identification and resolution inspection findings regarding licensee corrective action programs (CAPs), in the significance determination process (SDP) for operator requalification, and supplemental inspections that evaluate licensee root cause analysis. If implementation of the current maintenance rule was expanded to encompass periodic sampling of maintenance tasks in risk-significant non-safety grade systems, additional human performance issues might be identified. Additionally, event analysis conducted outside of the baseline inspection process has the potential to identify and characterize human performance issues not covered as part of the ROP.

A number of findings were produced from these analyses. These findings are described below.

- **General Finding.** The ROP can detect many of the human performance issues that can impact risk through its baseline inspections process, supplemental inspections, performance indicators, cornerstones, and crosscutting issues.

- **Risk Informed Inspection Notebooks.** Risk-informed inspection notebooks provide information on pertinent core damage scenarios that is necessary in the process to make a phase 2 evaluation of inspection findings. The notebook worksheets identify and provide order of magnitude estimates of successful performance of important operator actions in pertinent core damage scenarios. These estimates are based on licensee IPEs, which considered performance shaping factors. These shaping factors are considered in most probabilistic risk assessment (PRA) and human reliability analysis (HRA) analyses.

- **PIMs.** PIMs for four pilot plants revealed deficiencies in configuration management, CAPs,

engineering test and evaluation, inadequate post maintenance test, inadequate maintenance and actions, operator actions, knowledge and training, procedures and supervision. These are the same types of human performance issues found through operating event analyses.

- **Latent and Active Failures.** Previous work conducted by the INEEL identified a 4:1 ratio of latent to active errors contributing to operating events. The ratio of latent to active errors was 3:1 in ROP pilot and non-pilot inspection reports indicating a similar trend. The ROP does not currently follow a standardized approach to detecting and characterizing these latent factors.

- **Profile of Human Performance in the ROP.** Procedure deficiencies, configuration management deficiencies, and CAP deficiencies represent the majority of human performance issues identified in inspection reports. Operating events contain the same issues, and several others including design and maintenance issues. The findings from this study indicate that the ROP would not detect all of these deficiencies.

- **Relationship of Human Performance Issues in Events to the SDP.** To trigger the SDP, individual or trended human performance should challenge risk important systems. Many of the individual human performance risk-important contributors to operating events would not have triggered the SDP until combined with other human and hardware failures. Such information is not currently available to allow for trending of human performance issues that, by themselves, would fail to trigger the SDP.

- **Communications.** Communication factors were influential in events. Currently, other than through emergency preparedness evaluation, and observation of crew cooperation and communication during simulator exercises, the ROP does not directly assess aspects of communication.

- **Grouping of Human Error Categories.** Statistical analysis of operating event data demonstrated that 60% of operating events can be characterized by four groups of human error categories: (1) design and maintenance, (2) design, maintenance, and operations, (3) design, maintenance, and CAPs, and (4) operations, procedures, and CAPs. Many of the human errors involved improper maintenance of non safety-grade systems. Detection of these maintenance factors is unlikely without increased sampling of maintenance activities on safety-grade and non safety-grade systems.

- **Design Issues.** The ROP "design" cornerstone addresses the design issues found in operating events. However, there are two requirements to characterizing these issues. First, the systems with the underlying latent design failure are selected from a group of safety grade systems. Second, once a group of safety grade systems is selected, only a sample of these systems are subject to review. Thus, sampling and selection factors can reduce the likelihood of detecting safety as well as non-safety grade systems with underlying latent failures.

- **Respond to Industry Notices.** Twenty percent of operating events evidenced failures of utilities to respond to industry notices regarding equipment defects or the need for modified work practices. Currently, the means to detect such latent failures is through maintenance rule implementation and the Problem Identification and Resolution review conducted once per year by inspectors.

- **Corrective Action Program and Risk.** Operating event reviews indicate that deficiencies in licensee CAPs contributed to 41% of events. ROP guidance instructs inspectors to consider risk insights and risk importance in selecting corrective action deficiencies for review.

- **Diverse Errors Combine in Events.** Diverse human errors influenced the occurrence or severity of

operating events. The mechanisms by which various errors combine to produce failures are neither readily apparent nor easily modeled. These contributors to hardware failures and human failures that impact safety and non safety-grade systems, highlight the role of human performance as a crosscutting issue. Additionally, current HRA screening analysis procedures would potentially discard these smaller latent errors.

- **Training Issues Involving Non-Licensed Operators.** A number of Licensee Event Report (LER) event descriptions include failures by personnel other than licensed operators. The current ROP focus is primarily on licensed operators through the requalification SDP, but there is also a supplemental inspection on training that has broader applicability.

Procedural Inadequacies Contributing to Events. Thirty-eight percent of LER event descriptions contained evidence of procedural errors in design, construction, or compliance. These deficiencies primarily affected normal, abnormal, and maintenance procedures. Currently, procedures are indirectly assessed when work packages are reviewed, under the operator requalification SDP, during use of post-maintenance testing inspection procedures, during evaluation of surveillance testing inspection procedures, during the assessment of personnel performance during non-routine operations, or during corrective action plan review conducted under Problem Identification and Resolution. There are direct assessments of procedures using supplemental inspection for the quality of procedures and, as part of the human factors supplemental inspection, for the use and adherence to procedures.

ACRONYMS

AFW	auxiliary feedwater (system)
AIT	Augmented Inspection Team
ANO	Arkansas Nuclear One
ASP	Accident Sequence Precursor
ATHEANA	A Technique for Human Event Analysis
ATWS	anticipated transient without SCRAM
BWR	boiling water reactor
CAHR	Connectionism approach for Assessing the Reliability of Human Action
CAP	Corrective Action Program
CCDP	conditional core damage probability
CCF	common cause failure
CCP	centrifugal charging pump
CCTV	closed-circuit television camera
CDP	core damage probability
CFR	Code of Federal Regulations
CRD	control rod drive (mechanism)
CREAM	Comprehensive Reliability Analysis Method
CSIP	charging/safety injection pump
DER	deficiency report
EAL	emergency action level
ECCS	emergency core cooling system
EDG	emergency diesel generator
EFW	emergency feedwater (system)
EHC	electro-hydraulic control system
EOP	emergency operating procedure
ESFAS	engineered safety features actuation system
ESWS	essential service water system
FACE	Finnish Assessment of Commission Errors
FFD	fitness for duty
FRV	feedwater regulating valve
FSAR	final safety analysis report
HFIS	Human Factors Information System
HPCI	high pressure coolant injection
HPED	Human Performance Events Database
HPI	high pressure (safety) injection
HRA	human reliability analysis
I&C	instrumentation and control
IDS	Intrusion Detection System
IIT	Incident Investigation Team
INEEL	Idaho National Engineering and Environmental Laboratory
IPE	Individual Plant Examination

IPEEE	Individual Plant Examination of External Events
LCO	limiting conditions for operation
LDST	letdown storage tank
LER	Licensee Event Report
LOCA	loss of coolant accident
LOOP	loss of offsite power
MC	inspection manual chapter
MCC	motor control center
MERMOS	Human Factor Safety Mission
MPFF	maintenance preventable function failure
MORT	Management Oversight and Risk Tree (Analysis)
MOV	motor operated valve
MSIV	main steam isolation valve
MSSV	main steam safety valve
NCV	no color violation
NRC	Nuclear Regulatory Commission
NSS	nuclear shift supervisor
NUREG	Nuclear Regulatory Commission External Report
PA	protected area
PI	performance indicator, principal investigator
PIM	plant issues matrix
PORV	power operated relief valve
PRA	probabilistic risk assessment
PSA	probabilistic safety analysis
PWR	pressurized water reactor
QA	quality assurance
RCIC	reactor core isolation cooling
RCS	reactor coolant system
RES	Office of Nuclear Regulatory Research
RFI	risk factor increase
RHR	residual heat removal
ROP	reactor oversight process
RPS	reactor protection system
SALP	Systematic Assessment of Licensee Performance
SAR	Safety Analysis Report
SCRAM	safety critical reactor axe man
SCSS	Sequence Coding and Search System
SDP	Significance Determination Process
SER	Staff Evaluation Report
SPAR	Simplified Plant Analysis Risk
SRO	senior reactor operator
SRV	safety relief valve
SSC	structures, systems, and components

T_{ave}	average temperature
TDAFW	turbine driven auxiliary feedwater
TER	Technical Evaluation Report
TS	technical specification
UST	upper surge tank

Glossary

Baseline Inspection Program – Planned inspections performed at all nuclear power plants. The program will focus on plant activities that are not adequately measured by performance indicators, on the corrective action program, and on verifying the accuracy of the performance indicators. (SECY-99-007A)

Corrective Action Program (CAP) – The system by which a utility finds and fixes problems at the nuclear plant. It includes a process for evaluating the safety significance of the problems, setting priorities in correcting the problems, and tracking them until they have been corrected.

Crosscutting Area – Nuclear plant activity that affects most or all safety cornerstones. These include the plant's corrective action program, human performance, and the "safety-conscious work environment." (SECY-99-007A)

Finding – An observation that warrants further review within the significance determination process. (SECY-99-007A)

Inspection Reports – Reports are issued periodically to document inspection findings. These may cover a specific time period for the baseline inspection or a particular event or problem examined in a reactive inspection. All inspection reports are public documents and, when issued, are posted to the NRC's internet web site.

Observation – Any detail noted during an inspection. (SECY-99-007A)

Performance Indicator – Objective data that records performance in a specific cornerstone of safety at a nuclear power plant. (SECY-99-007A)

Plant Issues Matrix (PIM) – A consolidated listing of plant issues (i.e., inspection findings) in the Reactor Program System (RPS)used by NRC to assess plant performance (MC 0610).

Reactive Inspection – Inspections to examine circumstances surrounding an operational problem or event at a nuclear plant. (SECY-99-007A)

Regulatory Conference – A meeting between the NRC staff and a utility to discuss potential safety issues or to discuss a change in performance as indicated by a declining performance indicator or inspection finding. These meetings are open to public observation unless they cover security issues, NRC investigation findings, or similar sensitive topics. (SECY-99-007A)

Resident Inspector – An NRC inspector assigned to a nuclear plant on a full-time basis. Each site has at least two resident inspectors. (SECY-99-007A)

Risk-informed – Incorporating an assessment of safety significance or relative risk in NRC regulatory actions (SECY-99-007A)

Risk Informed Inspection Notebooks – Provide information on pertinent core damage scenarios that is necessary in the process to make a phase 2 evaluation of inspection findings, and are important tools for inspectors, insuring that inspections will be appropriately focused.

Cornerstone of Safety – Nuclear plant activities that are essential for the safe operation of the facility. These cornerstones are grouped under the categories of reactor safety, radiation safety, and safeguards. (SECY-99-007A)

Safety Conscious Work Environment – A working environment in which employees are encouraged to report safety concerns without fear of criticism or retaliation from their supervisors because they raised the issue. (SECY-99-007A)

Significance Determination Process – The process used by the NRC staff to evaluate inspection findings to determine their safety significance. This involves assessing how the inspection findings affect the risk of a nuclear plant accident, either as a cause of the accident or the ability of plant safety systems or personnel to respond to the accident. (SECY-99-007A)

Systems, Structures and Components (SSC) – Basic components of nuclear power plants

1. INTRODUCTION AND BACKGROUND

Human performance often manifests itself as the root cause of performance problems in nuclear power plants. Because of its potential impact upon safety, human performance is given consideration in the Reactor Oversight Process (ROP) as a crosscutting issue. In SECY –99-007, "Recommendations for Reactor Oversight Process Improvements," the technical framework task group sought to identify performance indicators as a means of measuring the performance of key attributes in each of the cornerstone areas.

The task group also identified aspects of licensee performances [such as human performance, the establishment of a safety conscious work environment, common cause failures, and the effectiveness of licensee problem identification and corrective action programs (CAPs)] that are not identified as specific cornerstones but are important to meeting the safety mission.

The task group concluded that these items generally manifest themselves as the root cause of performance problems. Adequate licensee performance in these crosscutting areas is inferred through cornerstone performance results from both performance indicators and inspection findings. It was hypothesized concerning human performance in the ROP that the effects of human performance on plant safety would largely be reflected in the plant performance indicators and inspection findings. As a means of testing this hypothesis, ROP guidance and findings were compared to findings for human performance in operating events.

1.1 Description of Technical Activities

The Idaho National Engineering and Environmental Laboratory (INEEL) was tasked to: (1) Review the Nuclear Regulatory Commission (NRC) Reactor Oversight Process and other information to identify and describe the means by which NRC monitors, analyzes, and feeds back information on human performance. Included in this review are aspects of the ROP including information sources, such as risk informed inspection notebooks, inspection reports, inspection manuals and procedures, and applicable supplemental guidance.

(2) Review other sources of human performance data to determine how human performance has contributed to operational experience. This review was performed using operating experience and insights from past analyses and studies in human reliability analysis (HRA), probabilistic risk assessment (PRA), and human performance. Included are the following:

- Accident Sequence Precursor (ASP) analyses;
- Sequence Coding and Search System (SCSS) results;
- Human Factors Information System (HFIS) data;
- Human Performance Events Database (HPED) reports;
- Incident Investigation Team (IIT) reports;
- Augmented Inspection Team (AIT) reports;
- Other relevant inspection reports.

(3) Compare the results of (1) and (2) above to determine if the ROP would have caught the main risk-important human performance contributors and the likelihood of the ROP identifying each contribution in the future.

(4) Develop a listing of the types of information on human performance that are only indirectly collected or considered by the ROP, and assess their safety significance.

Report Organization

Chapter 1 presents the introduction and background to the present report. Chapter 2 presents the overview and findings from the

review of human performance in operating events. Chapter 3 presents findings from the review of human performance characterization in the reactor oversight process. Chapter 4 contains findings from the comparison of the ROP human performance characterization with human performance in operating events presented in Chapter2. Chapter 5 discusses insights for human performance enhancement in the ROP.

2. HUMAN PERFORMANCE IN OPERATING EVENTS

2.1 Method and Scope

The method used to determine the risk impact of human performance in operating events is discussed in NUREG/CR-6753, 2001. A brief synopsis is presented here but interested readers are referred to that document for details.

In response to a need to better understand how human performance influences the risk associated with nuclear power plant operations, the U.S. NRC Office of Research (RES) requested the INEEL to identify and characterize the influences of human performance in significant operating events. The INEEL used the 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.

Fifty events at U.S. nuclear power plants were selected for study and review. Eleven events were determined to have little or no human performance influence and were not analyzed further. Of the remaining 39 operating events, 37 were analyzed qualitatively. Quantitative SPAR models exist for 23 of these events; SPAR models did not exist for the operating modes for the remaining 14 events. The latter have been the subject of qualitative analysis only.

Seven events were described in both AITs and Licensee Event Reports (LERs) analyzed by the ASP program; the remaining 30 events were only described in LERs. No general trends or differences were noted regarding the influence of human performance based on whether the source document reviewed was from an AIT or LER. Neither was there a discernible trend between AIT and LER events regarding the type of human performance problems noted, with the exception that AIT events often contained richer descriptions of errors or failures that occurred during events than did many of the LERs.

The first events selected for analysis had relatively high ASP conditional core damage probabilities (CCDPs) (i.e., on the order of 1.0E-4 to 1.0E-3). These were investigated by NRC and involved human performance. Of the 23 quantitative analyses performed, six were for boiling water reactors (BWRs) and 17 were for pressurized water reactors (PWRs). For the other 14 events, 2 qualitative analyses were performed for BWRs, the remaining 12 qualitative analyses were performed for PWRs. A team consisting of a plant systems/SPAR analyst, a human factors/human reliability analyst, and a plant operations analyst reviewed the events and reached consensus regarding performance influences. Based upon work by Reason (1990), influences were characterized as either latent (i.e., having occurred earlier but influencing the event in some manner) or active (i.e., having functioned as either the initiator or otherwise influenced mitigation or recovery action in some manner). As a result of the analyses, a number of quantitative results and human performance insights were obtained.

A link was clearly demonstrated quantitatively and qualitatively between human performance and risk. For 13 of 20 events, the dynamic range for the risk factor increase (RFI)[1] was from 5 to 24,500. Human performance was a significant contributor to these increases in risk, as measured by the RFI.

The calculated CCDPs present in Table 2-1 ranged from a high of 5.2E-3 to a low of 2.6E-05. Event importance [i.e., CCDP – core damage probability (CDP)] scores ranged from a low of 1.0E-6 at Millstone 2 (1995) to a high of 5.2E-03 at Wolf Creek (1996). Events resulting in CCDPs greater than 1.0E-4, such as Clinton (1995) and Oconee Unit 2 (1992), contained failures not unlike those present in events with lower CCDPs. There was a strong human performance contribution to these events (i.e., ranging from 10 to 100%). Risk measures

[1] The RFI is the event CCDP divided by the nominal (base) case core damage probability (CDP). The CDPs are SPAR peer-reviewed baseline PRA models; the CCDP is a reflection of the event scenario being evaluated.

such as the risk factor increase had similar findings. For example, there was no tendency for events with a higher RFI to have more or less human performance involvement than those with a lower RFI.

Human Error Category Coding

Human error categories and subcategories were empirically derived from a review of LER data, AIT reports, and other information sources. They are based upon frequency of occurrence in report sources. Based upon current HRA practices (See Reason 1994) failures were further divided into "active" or "latent" failure modes. A two-tiered human error category coding method was utilized in the original assessment of the event data. The first tier is comprised of six categories listed below:

Human Error Coding Tier 1

1. Operations
2. Design and Design Change Work Practices
3. Maintenance Practices and Maintenance Work Control
4. Procedures and Procedures Development
5. Corrective Action Program
6. Management and Supervision

Second Tier. Upon further review of the raw event data, 21 error subcategories were generated for coding events. Every event was individually evaluated for the presence of these 21 error subcategories. These subcategories are listed below. Table 2-2 presents the assignment of the 270 errors identified in the coding process for events to the individual subcategories presented below.

Human Error Subcategory Coding – Tier 2

1. Command and Control Including Resource Allocation
2. Inadequate Operation Knowledge or Training
3. Incorrect Operator Action/Inaction
4. Communications
5. Design Deficiencies
6. Design Change Testing
7. Inadequate Engineering Evaluation
8. Ineffective Abnormal Condition Indication
9. Configuration and Configuration Management
10. Work Package Development, Quality Assurance (QA) and Use
11. Inadequate Maintenance Work Packages and Work Practices
12. Inadequate Maintenance Technical Knowledge
13. Inadequate Post Maintenance Testing
14. Inadequate Procedures and Procedures Development
15. Failure to Respond to Industry and Internal Notices
16. Failure to Follow Industry Practices
17. Failure to Identify by Trending and Use Problem Reports
18. Failure to Correct Known Deficiencies
19. Inadequate Supervision
20. Inadequate Knowledge of Systems Management and Plant Dependencies
21. Organizational Structure

2.2 Detailed Human Performance Findings

The range of human performance contribution to the event risk increase from the PRA base case was from a low of 10% to a high of 100%. The average contributor was 62%. Eighty-one percent of events, see table 2-2, showed evidence of human error in the "design and design review process," 76% of events contained human error in "maintenance practices and maintenance work control," and 54% of events contained evidence of "operations errors." Most events contained multiple errors that were not individually significant but were collectively significant. Detailed descriptions of errors from these individual events are presented in Appendix B. These failures formed the basis of human performance information that was compared with the ROP guidance and inspection report findings. Definitions of the 6 error categories and 21 error subcategories developed in this study are presented in Appendix C of this report. The relative error frequencies presented in Table 2-3 follows the same general trend as the findings discussed above regarding

Table 2-1. 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[2]
1	2.1E-04	Wolf Creek 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	2.3E-04	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

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

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

Category Description (Count/% of Total)	No. of Latent Errors	No. of Active Errors
Operations (72/27%)		
Command and control including resource allocation	4	14
Knowledge or training	15	8
Operator Action/Inaction	3	13
Communications	9	6
Design and Design Change Work Practices (71/26%)		
Design deficiencies	25	
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	
Procedural Design and Development Process (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 (10/4%)		
Inadequate supervision	7	1
Inadequate knowledge of systems and plant operations	1	
Organizational structure	1	
Subtotals	220	50
Total = 270/100%		

the presence of particular error categories in events. The exception is that there were more operations errors present than maintenance errors on a relative frequency versus an event basis.

2.3 Profiles Developed through Cluster Analysis

2.3.1 Profile Determination

Analyses were conducted to determine whether there were common groupings of human errors present during events. Statistical cluster analysis was performed based upon the six error categories. This analysis identified four groupings that accounted for 60% of the events reviewed in this study. Table 2-4 identifies the events associated with the four profile groups. Three of the four profile groups contained maintenance and design errors. The first event

group contained a core of design and maintenance errors; the second contained a core of design, maintenance, and operation errors. The third group contained five events with design, maintenance, operations and CAP errors, and the fourth grouping contained four operating events with operations, procedures, and CAP errors. In a number of instances, multiple errors were associated with the same system, e.g., the maintenance work package and worker

Table 2-4. Event Groupings Obtained Using Cluster Analysis

Group 1 – Design and Maintenance	Group 3 - Design, Maintenance, Operations, Corrective Actions
Catawba 1996	Arkansas Nuclear 1 1996
Comanche Peak 1995	Dresden 3 1996
Limerick 1 1995	Fort Calhoun 1992
Oconee 1, 2, & 3 1992	Haddam Neck 1993
Robinson 1992	McGuire 2 1993
Group 2 - Design, Maintenance, and Operations	**Group 4 – Operations, Procedures, Corrective Actions**
Beaver Valley 1 1993	Indian Point 2 1999
Calvert Cliffs 2 1994	Oconee 3 1997
Catawba 1993	Salem 1 1994
Oconee 2 1992	Wolf Creek 1994
River Bend 1994	
Wolf Creek 1996	

knowledge for industry practices regarding breaker maintenance were both lacking, leading to human errors that caused or contributed to breaker failures.

In all events, latent factors conditioned the events by providing an unanticipated context and complicating plant conditions. Features of each event group are presented and are discussed in terms of how human performance elements found in the profile may be addressed through the ROP.

Group 1

This group included a core of design and maintenance errors. These errors are summarized below.

Group 1 – Design and Maintenance Insights

- Errors were generally related to design and maintenance on the same equipment, component, or system;
- Work package and design problems were a factor in the majority of these events;
- Errors were primarily latent;
- Errors affected plant equipment outside the control room;
- Events occurred at different power modes and at different times of day;
- Concurrent failures occurred.

Operations errors did not play a role in these events.

Applicable Inspection Procedures - Design and maintenance issues are covered by the following

NRC inspections: (1) Safety System Design and Performance Capability, (2) Equipment Alignments, (3) In-service inspection activities (4) Maintenance Rule Implementation, (5) Maintenance Risk Assessment and Emergent Work Evaluation, (6) Post maintenance testing and (7) Surveillance Testing, and (8) Temporary Plant Modifications.

Group 2

The second event group contained six significant operating events. This group also contained aspects of maintenance and design errors. What made this group of events unique from the other groups was the inclusion of Operations errors. Design and maintenance errors are discussed in the Group 1 discussion. The insights from operations errors in Group 2 events are presented below.

Group 2 - Design, Maintenance, and Operations Failure Insights

- There were almost twice as many latent errors as active errors;
- Control room knowledge regarding activities conducted outside the control room in the majority of events was inadequate;
- Operations-related communications deficiencies existed in most of these events;
- All events occurred at power, implicitly making these failures serious;
- Active errors primarily involved licensed operators;
- Concurrent failures occurred.

Applicable Inspection Procedures - Design and maintenance issues are covered by the same inspections as Group 1.

Operations specific errors could be identified by the following: Licensed Operator Requalification Evaluation, Personnel Performances During Non-routine Plant evolutions, and Operator Work-Arounds.

Group 3

This group of events also contained aspects of maintenance and design errors. What made this group of events unique from the other groups was the presence in each event of both operations and CAP errors. The insights from CAP and operations errors are presented below.

Group 3 - Design, Maintenance, Operations and CAP Insights

- Errors in correcting known deficiencies were present in half of these events;
- Failure to trend problems were found in over half of these events;
- All involved equipment failures that occurred outside the control room;
- All but one event occurred at power;
- Operations induced equipment failures were both active and latent.

Applicable Inspection Procedures - Design and maintenance issues are covered by the same inspections as in Group 1.

Operations specific errors could be identified by the same inspections as Group 2.

CAP Failures are covered by: (1) Identification and Resolution of Problems, and (2) Supplemental Inspection Guidance for Root Cause Nos.95002/0023.

Group 4

This group contained concurrent operations, procedures and CAP errors. There was no discernable pattern regarding human errors in terms of design or maintenance. The insights from the pattern of operations, procedures, and corrective action errors are presented below.

Group 4-Concurrent Operations, Procedures, and Corrective Action Program Insights

- These events occurred while the plant was at different power modes (e.g., at power, shutdown, and shutting down);
- Control room errors were committed;

- Command and control problems were evident for all events in this group;
- Inadequate knowledge and training of operations personnel contributed to most events;
- Procedural deficiencies were identified in operations, maintenance and emergency activities;
- Procedures were either inadequate or non-existent for some activities;
- Failures to correct pre-existing, known deficiencies were present in most events.

Applicable Inspection Procedures - Concurrent operations could be identified by NRC inspections: (1) Licensed Operator Requalification Evaluation, and (2) Personnel Performance During Non-routine Plant Evolutions. Maintenance procedure deficiencies could be identified by (3) Maintenance Rule Implementation or by deficiencies noted during (4) Post maintenance testing.

CAP Failures could be identified by (5) Identification and Resolution of Problems.

2.3.2 Findings

Findings regarding the influence of human performance on risk are summarized below.

Effect of Human Performance

Human performance was found to be a major contributor to the risk increases in significant operating events. Since the events were selected on the basis of human performance involvement, there is some bias present. In the samples studied, SPAR models have shown increases ranging from 10% to 100%. The average contribution to events was 62%.

Latent Errors

Latent errors from a variety of sources were important and significantly affected events. Latent contributions to events were noted more than active contributions by a factor of four. This is similar to other recent studies (Reason 1998; Gertman *et al.*, 1998). Latent failures were noted in all facets of performance studied.

Combining of Human Performance Problems

All operating events involved multiple human failures. Events such as loss of offsite power (LOOP) or loss of coolant that challenged the plant contained a concatenation of failures. On average, the 37 events contained 4 or more errors in combination with hardware failures. 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 QA during procedure writing, duties and responsibilities not clearly understood during events, failure to trend and address previous problems, errors in maintenance practices, and failure to test after equipment malfunctions. For active contributory errors, the important factors included command and control, correctness of actions, and adequacy of supervision. INEEL findings regarding the risk impact of human error in operating events notes examples of many errors mapping to single PRA basic event (NUREG/CR-6753). It would be beneficial to develop an understanding of the common cause mechanisms underlying human–human and human–system dependencies. In some instances, human error influenced subsequent errors. In other instances, errors influenced a basic event that contributed to subsequent basic events in the PRA model.

In general, failure rate information regarding the concatenation of smaller failures into events is non-existent. It would also be beneficial to determine the linkages between these failures and to generate failure rates for use in HRA and PRA.

Recurrent Problems

Many events evidenced licensee failures to monitor, observe, or otherwise respond to negative trends, industry notices, or design problems. This suggests that weaknesses in licensee CAPs may play an important role in influencing operating events.

Relationship to Individual Plant Examination

(IPE)

The IPEs (see NUREG-1560) primarily account for human contributions to plant risk through operator actions in response to upset plant conditions. This is a legitimate source of risk. For example, three common event sequences segments were determined to be important in all PWR analyses: (1) switch to recirculation, (2) feed and bleed, and (3) depressurization and cool down. In this study, latent maintenance failures such as maintenance and work process factors were identified as important sources of risk in operating events. The extent to which these latent failures contributed to plant risk is not well documented in IPEs.

2.4 Mapping of Events to Inspection Procedures

An attempt was made to show how performance findings from events might be identified using ROP guidance. Four events identified with high ASP program CCDPs were selected and reviewed: Comanche Peak (1995) loss of feedwater leading to reactor trip event, Catawba (1993) emergency service water unavailability event, Haddem Neck (1993) logic tests leading to LOOP event, and Fort Calhoun (1992) reactor high pressure trip and loss of coolant accident (LOCA). In general, existing baseline and supplemental procedures have the potential to detect the deficiencies that contributed to these events. Details of the mappings are presented in Appendix D.

There were applicable Inspection Procedures for all four events. They included personnel performance during non-routine evolutions, safety system design and performance capability, emergency preparedness, operator requalification, maintenance rule assessment and emergent work, and equipment alignment.

It should be noted that the existence of the inspection procedure (IP) does not guarantee that the systems involved in these events would either be selected or sampled as part of the inspection process. This could potentially apply to non-safety grade but safety-important systems.

Performance Indicator (PI) findings.

All four events reviewed contained evidence of design inadequacies. There was no applicable PI for this attribute. All four events also contained evidence of inadequate maintenance practices or surveillance problems. The applicable PI for these was safety system functional failures.

2.5 Discussion

For the majority of events, the analysis of raw event data and event group data identified deficiencies in design and maintenance work practices. Such failures are almost entirely latent, preceding the operating event in time. Hence, they may also be detectable before an event occurs. Since the core of most operating event profiles involved design and maintenance failures, emphasis of aspects of the inspection processes that could potentially enhance detection of such failures may be important for reducing certain kinds of events, or at least reducing their severity.

Shortcomings in licensee CAPs were also observed in many operating events. Such programs are reviewed as part of the ROP guidance through implementation of the Inspection Procedure for Problem Identification and Resolution.

In some events, the technical knowledge of operators and maintenance personnel was judged to be weak regarding systems that were contributors to the events. Currently, defects in operator knowledge would be detected through the Operator Requalification Evaluation Inspection Procedure. Maintenance problems are generally determined through implementation of the maintenance rule, but may also be detected through evaluation of post maintenance testing and inspection for surveillance testing.

The NRC has inspection modules in many areas in which deficiencies in performance were identified in this study (See section 3.0). The results from the INEEL review of events may serve to inform future revisions of such

inspection modules to improve upon their ability to identify such deficiencies before they have the opportunity to contribute to future operating events.

Most of the ASP events analyzed in this study contained elements that were related to human performance and failures in work processes. These human performance elements, in conjunction with other failures, contributed to significant increases in plant risk over the nominal, base case risk estimates. In nearly all cases, a number of latent errors combined with concurrent hardware failures and active human errors to produce these risk increases. Although in every event operators were ultimately successful, failures caused by multiple latent errors complicated diagnosis, response planning, and mitigation efforts.

The HRA methods used in IPEs are not well suited to identifying or modeling the complex latent errors that occurred in these events. As part of efforts that address future HRA needs, a more explicit consideration of latent failures and mechanisms by which they combine could aid in event interpretation and support improvement in HRA modeling and quantification action. Additionally, because the way in which small errors combine is not well understood, many screening analysis approaches would discard these latent errors.

3. HUMAN PERFORMANCE IN THE REACTOR OVERSIGHT PROCESS

3.1 Introduction

Human performance in the ROP is considered within the broad framework of reactor safety, radiation safety, and reactor safeguards evaluation. Evaluation of licensee performance is achieved through assessment and consideration of seven safety cornerstones, three crosscutting issues, and 20 performance indicators. A complete overview of the ROP is contained in SECY – 99 – 007A.

3.2 Program Elements

Guidance is provided in the form of baseline inspections, supplemental inspections and the significance determination process (SDP). The cornerstones, crosscutting issues and performance indicators, baseline inspections, supplemental inspections, and the SDP are discussed briefly below.

3.2.1 Cornerstones

The cornerstones supporting the reactor oversight process consist of initiating events, mitigating systems, barrier integrity, emergency preparedness, occupational radiation safety, public radiation safety, and physical protection.

3.2.2 Crosscutting Issues

The three crosscutting issues associated with reactor safety are human performance, a safety-conscious work environment, and a CAP.

3.2.3 Performance Indicators (PIs)

PIs are a basic performance measure that form part of the technical basis of the ROP. A listing of these indicators is presented in Appendix A. The objectives of the performance indicator process are:

1. Improve objectivity of the oversight process;
2. Improve the scrutiny of the NRC assessment process so that it is more closely tied to licensee performance; and
3. Risk-inform the regulatory assessment process so that NRC and licensee resources are focused on aspects of performance having the greatest impact on safe plant operation (NEI 99-02 Rev 0).

Performance indicator reports are submitted to the NRC for each power reactor unit. Information describing these process factors is found on the NRC web site.

3.2.4 Baseline Inspection Process Manuals, Procedures, and Reports

Inspection manuals and procedures define guidance for implementing the ROP. These documents were reviewed to aid in understanding how the ROP characterizes human performance. The INEEL research team identified a number of procedures and supporting documents. Those most important to human performance are summarized below.

3.2.4.1 Inspection Reports

Inspection reports (IRs) are one means by which the NRC assesses and monitors human performance. Inspection findings for each plant are documented in IRs in accordance with Inspection Manual Chapter (MC) 0610 and summarized in plant issues matrixes (PIMs). (Examples of PIM findings and issues are presented below.) A sample of active and latent human errors documented in IR findings is available in Tables E-1 and E-2 of Appendix E.

Review of these findings is presented in Chapter 4.

3.2.4.2 SDP for Operator Requalification (NUREG 1021 – Rev 8)

This SDP provides the green, white yellow and red determinations for the annual operator requalification examinations. The process follows the criteria of NUREG 1021 Rev. 8, for the Operator Requalification Program. The SDP is thorough. Human performance issues that may challenge plant safety are entered into the utility CAP. The PI rules require that entry into the licensee program occurs for Green and above findings. If, 1/3 of crews fail, a "green finding" is issued and entered in the CAP. If a failed crew is returned to shift without remediation, the issue becomes white. The operating events INEEL reviewed revealed that both concurrent activities and the status of ex-control room equipment proved challenging for crews. Changes in scope and realism offered to crews including representing complicating plant conditions such as ex-control room activities and concurrent failures may provide opportunity to approximate conditions observed during events.

3.2.4.3 Plant Issues Matrix and Inspection Report Review

Inspections are performed by NRC resident inspectors stationed at each nuclear power plant and by inspectors based in one of the four NRC regional offices or in NRC headquarters. The inspection program uses a risk-informed approach to select areas to inspect within each cornerstone. The inspection areas were chosen because of their importance in terms of potential risk, past operational experience, and regulatory requirements (NUREG-1649, p. 5). This process replaces the assessment process previously conducted under the Systematic Assessment of Licensee Performance (SALP) program.

The human performance information contained in these reports has the potential to call attention

to indicators and trends prior to their combining to trigger the SDP. Each may not be risk significant in itself but may highlight underlying conditions and mechanisms by which smaller, often latent failures can combine to initiate or complicate operating events.

3.2.4.4 MC 0609 Significance Determination Process

The SDP provides a means by which to characterize the significance of an inspection finding consistent with the NRC regulatory response thresholds used for performance indicators, provides an objective framework for communication, and provides a basis for enforcement actions associated with an inspection finding. The SDP does not relieve the licensee from compliance with technical specifications or other regulatory requirements.

MC 0609 differentiates between findings and observations. Observations are any detail noted during an inspection. Findings are observations placed in context that have been determined to warrant more detailed review using the SDP. The characterization of the significance of a finding employs the SDP outcome color scheme to identify the level of significance. The output of each cornerstone SDP process serves as an input to the assessment and or enforcement process.

MC 0609 presents criteria for determining an issue's status (i.e., whether or not the issue is minor). Many of these issues involve human performance considerations because they involve subjective judgment on the inspector's part or implicitly or explicitly involve review of human performance issues on the licensee's part. These criteria include:

- Does the issue suggest a programmatic problem that has a credible potential to impact safety;
- Could the issue be viewed as a precursor to a significant event; and
- If left uncorrected, would the same issue become a more significant safety concern?

A second group of questions is also used and if any answer is "yes," then the issue is subject to analysis by the SDP method:

- Could the issue affect the operability

availability, reliability, or function of a system or train in a mitigating system; and
- Could the issue involve degraded conditions that concurrently influence any mitigation equipment and or initiating event?

A third group of questions in MC 0609, implemented when extenuating circumstances have been determined includes the following:

- Does the issue involve willfulness;
- Does the issue provide substantive information regarding crosscutting issues; and
- Is documenting this issue necessary to close an open item from an LER or allegation?

Guidance specifies three phases for significance determination. They are characterization and initial screening, initial risk significance approximation and basis, and risk significance finalization and justification. Plant-specific inspection notebooks are used to support this process. Notebooks used by inspectors contain a number of event sequence information worksheets that consists of simplified event trees called SDP event trees used to describe accident sequences. For example, Brunswick (GE BWR Mark I containment design plant) SDP event trees contain transients, small LOCA, medium LOCA, large LOCA, LOOP and anticipated transient without SCRAM (ATWS).

The objective of the SDP is to identify those "at power" core damage accident sequences whose likelihood is increased due to the conditions described in the inspection finding. For bounding conditions, a worst case condition, e.g., complete loss of function, is often assumed.

Treatment of human performance

Operator recovery from undesired plant conditions is explicitly considered as part of the SDP. Recovery Step 2.3.2, "Operator recovery actions," are included as part of the SDP worksheet process. The inspector, given the availability of equipment, is to determine if the nature of the degradation is such that an operator could recover the unavailable equipment or function in time. Operator action assumptions are to be documented by the inspector. Overall, the conditions considered in this review of operator recovery are comprehensive.

Inspectors review operator recovery actions against five criteria:

1. Sufficient time is available to implement recovery actions;
2. Environmental conditions allow access where needed;
3. Procedures exist;
4. Training is conducted on existing procedures under conditions similar to the scenario; and
5. Any equipment needed to complete actions is available and ready for use.

Differentiation is made between post initiator operator actions conducted under conditions of high and low stress. For example, when operators must manually open 2 out of 7-safety relief valves (SRVs) during an event, this activity is considered to be an operator action conducted under high stress. In guidance regarding this type of operator action taken under high stress, where the operator is providing mitigation, the operator response is assumed to have a failure probability of 1.0E-1. Recovery of a failed train can be inside or outside of the control room, but when credited in the model as a remaining mitigation capability, it is to receive a 1.0E-1 probability of failure. Operator actions with sufficient time are credited as 1.0E-3.

Screening is also conducted to determine the potential contribution to external events and follows the utility Individual Plant Examination of External Events (IPEEE). This is input to the Phase 3 analysis. Staff evaluation reports (SERs) and technical evaluation reports (TERs) are completed based upon IPEEE, and contain condensations of risk insights helpful to inspectors.

The plant specific scenarios from PRAs guide selection of applicable scenarios that are provided to inspectors in the form of Phase 2 worksheets. In addition, the inspectors can

consult technical specification bases, Safety Analysis Reports (SARs), and emergency operating procedures (EOPs).

3.2.5 Supplemental Inspection Procedures

Supplemental inspection procedures are used to further evaluate significant performance issues identified either by inspection findings evaluated using the significance determination process or when performance indicator thresholds are exceeded. When an inspection finding is categorized as risk significant or when a performance indicator exceeds the "licensee response band" threshold, the NRC regional office will perform supplemental inspection(s). The NRC's assessment "Action Matrix" and Supplemental Inspection Table provide guidance regarding the scope and breadth of these inspections.

3.2.5.1 Supplemental Inspection Procedure for Root Cause Analysis (IP 71841)

Supplemental inspections of root cause are performed as a result of risk significant performance issues and are applicable across all cornerstones. If the licensee's evaluation of the performance issue is weak they can be subject to additional agency action. Also, weaknesses in the licensee's program can be documented in the inspection report. This supplemental procedure is invoked only after the SDP threshold has been exceeded. It serves as a check on what has been determined to be the root cause by the licensee and is not a procedure to verify that all the identified root causes and contributory causes have been completely identified. Language in the SDP implies that licensees with superior CAPs may be subject to less scrutiny than plants with inferior or flawed CAPs.

A number of root cause analysis methods that the licensee may identify for use are included in the IP. These include event and causal factor analysis, fault tree analysis, barrier analysis, change analysis, management oversight and risk tree analysis (MORT) and critical incident technique. Evaluation by the licensee should also include timely data collection, preservation of evidence, and determination of cause and effect relationships including potential hardware, process, and human performance issues.

The supplemental Inspection Procedure IP 71841 "Human Performance," is to be performed in conjunction with Supplemental Inspection Procedure 95002, "Inspection for One Degraded Cornerstone or Any Three White Inputs in a Strategic Performance Area." The IP is comprehensive and uses NUREG/CR-0700, Rev. 1, and 10 CFR Part 26, *Fitness for Duty*, as sources. It covers human performance issues as causal factors across all seven cornerstones. The major topic areas include visual information, control functions, alarms, and environmental factors. Human performance causal factors also include communication, work supervision and work practices, training and procedural adherence. This procedure is relatively new and at the time of this report it was not possible to review data resulting from the application of this particular supplemental inspection guidance.

3.2.6 Maintenance Rule Implementation (71111.12)

The maintenance rule covers functional failures as well as the monitoring and documenting of availability and reliability for structures, systems, and components (SSCs). The goal for inspectors is to inspect approximately six safety systems and components each calendar quarter.

Inspectors are to verify that the licensee identifies issues related to this inspection area at an appropriate threshold and enters these issues into the CAP. Inspectors are assigned 54 hours per quarter, or approximately 216 hours per year. A separate periodic review should take 40 hours and is to be carried out every 2 years. The region may also be involved in the periodic review process.

The maintenance rule guidance specifies that inspectors are to review the licensee's problem identification and resolution of maintenance rule-related issues. The inspectors also verify that low safety significant standby SSCs are being

monitored at least at the train level for availability and reliability.

For example, if an SSC suffered a functional failure, the NRC will evaluate it to determine if it was a maintenance preventable function failure (MPFF) or not. Examples of functional failures caused by maintenance include operator misalignments, maintenance procedure errors, and improperly performed surveillance.
If the SSC was a MPFF, then the licensee is to determine if it was a repetitive functional failure. References cited in the guidance above include NUMARC 93-01 and 10 CFR 50.65 (a)(1). For SSCs classified as part of (a)(1) of the rule, the inspector must verify that the licensee:

- Has taken appropriate corrective action;
- Has established goals commensurate with safety;
- Is monitoring the performance or condition of SSCs against licensee-established goals in a manner to provide reasonable assurance that SSCs are capable of performing their mission;
- Has determined whether SSC performance remains bounded by (a)(2) of the maintenance rule performance criteria.

3.2.7 SECY–00-0049, "Results of the Revised Reactor Oversight Process Pilot Program" Dated February 24, 2000

This document describes experiences from resident inspectors and other stakeholders, which are summarized below:

- Inspectors considered the revised program to be an improved oversight approach. However, in their opinion, additional improvement was needed for crosscutting issues (in general), the SDP, and enhanced monitoring of the licensee's CAP. There was some concern expressed about the need for clarification regarding a number of PIs and their thresholds.

- Stakeholder concerns with the ROP were:
  1) resource estimates for many of the individual inspection procedures were too low;
  2) the scope and frequency defined for certain inspection procedures is designed to account for site specific differences; and,
  3) the program needs to more clearly define the role of crosscutting issues such as human performance.

As a result, guidance for IPs was changed to allow inspectors to document pertinent observations that relate to important cross-cutting areas but that do not readily lend themselves to evaluation through the SDP.

4. HUMAN PERFORMANCE FINDINGS AND RECOMMENDATIONS

4.1. Characterization Present in the ROP

The working hypothesis for this effort was that the ROP identifies the same human performance issues that were identified through analyses of operating events. It was further hypothesized that the effects of human performance on plant safety would largely be reflected in the plant performance indicators and inspection findings. No hypothesis was made as to which part of the ROP reporting process would identify these human performance issues. Findings from INEEL's review of the ROP indicate that the ROP has demonstrated the ability to capture a number of human performance findings similar to those observed in operating events. Within the context of a risk-informed approach, however, a number of human performance issues are more challenging to identify than in a deterministic approach. Recommendations regarding identifying and including human performance issues that are less discernable in the ROP are presented in the summary section of this Chapter and in Chapter 5.

INEEL reviewed inspection reports, summary inspection reports, and plant issues matrices for evidence of human performance identification and characterization within the ROP. A description of this review follows.

The NRC had identified nine plants from four regions for pilot testing of the new reactor oversight process. These are referred to as pilot plants. The INEEL sampled four of these plants, one from each region. Human performance highlights from this sample pilot application are discussed below. Findings from 16 non-pilot plants were also reviewed and discussed. Tables E-1 and E-2 in Appendix E display performance failure category frequencies for these pilot and non-pilot facility inspection reports respectively. Comparison of pilot and non-pilot plants are discussed in subsequent sections. Note that the small sizes of samples may also be a factor in the comparison findings.

4.1.1 Review of Inspection Reports

An initial sample of 4 pilot and 16 non-pilot plant findings was reviewed for evidence of human performance characterization. The four pilot plants reviewed were Fitzpatrick, Cooper Nuclear Station, Sequoyah 1&2, and Prairie Island. The inspection reports reviewed covered the period 1999 through 2000. Descriptions in these reports suggests that the ROP as implemented: (1) is successful in terms of identifying a broad number of performance issues where the SDP has not been triggered; and, (2) provides evidence of NRC inspectors applying existing guidance to address human performance.

Trends were identified for pilot and non-pilot plants. Both pilot and non-pilot plant samples involved many instances of procedure deficiencies and failure to follow procedures. Procedures were present in 22% and 25% of findings, respectively. Configuration management problems including equipment configuration were present for 14% of total issues for pilot plants and only 8.3% of issues for non-pilot plants. This difference may be due to sampling error, relatively small samples were used. The largest difference determined between the samples was the involvement of corrective action plan deficiencies. In the non-pilot sample, 29% of findings were related to corrective action plan deficiencies. In the pilot plant sample, CAP issues comprised 11% of the total findings. Again, greater resources and scrutiny of the pilot plants may have resulted in these plants addressing a greater number of corrective action items.

In the non-pilot sample, 12.5% of findings related to failure to perform operability testing or deficiencies in performing that testing; these deficiencies were 6% of the findings for pilot plants sampled. Forty of the human performance issues identified in the pilot plant inspection reports involved combinations of procedure deficiencies (or deficiencies in their

use), configuration management problems including equipment configuration, and CAP failures. In all but two instances, these issues failed to trigger the SDP process. Thus, the inclusion of these issues in reports may have the potential to highlight industry-wide and individual plant issues or trends before they affect risk.

4.1.2 Review of PIMs Findings

A sample of four PIMs from pilot plants was reviewed for evidence of human performance characterization. Findings are presented below. In general, these findings are a rich source of human performance characterization. Almost all are "no color" findings that would fail to trigger the SDP. Nine of the twenty-one subcategories for human performance described in Table 2-3 of this report were identified in the four PIMs. These PIM findings are grouped below by subcategory.

4.1.2.1. PIMs - Configuration Management

- Delays were noted in ensuring that relevant information was communicated to operators (Fitzpatrick);
- The licensee failed to control the fire protection system configuration. A long standing degradation in which a required drain plug was missing, resulting in degraded effectiveness of CO_2 (Fitzpatrick);
- The licensee failed to control high pressure coolant injection (HPCI) system configuration. Twenty-five discrepancies were identified during walkdowns conducted within a single safety system. There was a lapse of control and excessive time (2 weeks) was taken to enter discrepancies into the CAP (Fitzpatrick);
- Configuration management failed to control the accuracy of a fire suppression system electrical design drawing (i.e., fire detectors were wired such that they would actuate the wrong suppression valves and no water would be supplied). (Sequoyah 1&2).

4.1.2.2 PIMs - Corrective Actions and CAP

- Weaknesses were noted in entering items into the corrective action system (Fitzpatrick);
- The licensee failed to take appropriate corrective actions. This occurred following an NRC-identified deficiency in regard to operators not complying with written operating procedures (Fitzpatrick);
- The licensee failed to initiate a deficiency report (DER) for a safety bus control power fuse block clip in violation of NRC requirements and station procedures (Fitzpatrick)
- Licensee management understood the causes of poor engineering performance; however, the causes were not corrected (Cooper);
- Self-assessment failed to emphasize the effect of the engineering backlog or design issues associated with a DC voltage system (Cooper);
- Licensee failed to promptly identify and correct problems with the calibration of ultimate heat sink instrumentation. (Sequoyah 1&2)

4.1.2.3 PIMs - Engineering Test & Evaluation

- Weaknesses in testing the HPCI systems contributed to system unavailability (Fitzpatrick);
- System walkdowns failed to detect a number of material condition issues (Fitzpatrick);
- The licensee failed to perform independent engineering verification regarding a reactor water level response test. Two levels of plant management failed to notice or correct the issue until prompted (Fitzpatrick);
- The turbine driven auxiliary feed water pump maintenance rule was misinterpreted. There were previous maintenance rule violations [e.g., failure to classify the failure as a functional failure under criterion 1(a)] (Sequoyah 1&2);
- The licensee inappropriately reclassified safety-grade pumps to non-safety grade (Prairie Island);
- Engineering failed to consider the

increased failure rate of the auxiliary feedwater (AFW) system associated with a pump trip on low suction pressure due a recent pump modification (Prairie Island);
- Engineering failed to properly consider the effect of the design change that violated Criterion III of 10 CFR. (Prairie Island)

4.1.2.4 PIMs Inadequate Post-Maintenance Test Including Calibration

- The licensee failed to adequately establish core spray timer calibration. Although there was excessive time delay, the diesels and core spray would have performed their intended function (Fitzpatrick);
- During a post maintenance test, a circulating lube oil pump for the emergency diesel generators (EDGs) and relays failed (Fitzpatrick);
- Plant personnel failed to adequately test the permissive for the fast opening feature of the turbine bypass valves. (Cooper)

4.1.2.5 PIMs –Inadequate Maintenance Practices

- On two occasions, maintenance personnel failed to follow maintenance procedures when working on a control rod drive (CRD) flow control valve (Cooper);
- Maintenance personnel constructed a scaffold in the auxiliary building that blocked the operation of a secondary containment isolation valve (Cooper);
- Torus vacuum breakers failed an as-found test. The valve seats had been incorrectly assembled during the previous refueling outage. The work package left complicated steps to "skill of the craft" and did not provide sufficient acceptance criteria (Cooper);
- In 1999, control room habitability was questioned when inspectors observed a broken door leading to the control room chiller room (Prairie Island);
- The licensee improperly secured Unit 1 sump hatches that are located directly under the reactor vessel. The issue was assessed as a not-cited violation (Prairie Island);
- Inspectors identified that a cooling water line was not adequately protected from freezing. As a result, ice formed in the cooling water emergency dump to grade line due to a leaking isolation valve. (Prairie Island)

4.1.2.6 PIMs - Operations

- Operators armed and withdrew a control rod after determining that the rod was inoperable (Cooper);
- Plant personnel erroneously declared the reactor equipment cooling system operable based on misinterpretation of NRC enforcement discretion (Cooper);
- There was a failure to perform an operability evaluation of a reactor recirculation pump discharge isolation valve (Cooper);
- During an excess draining event, it was noted that operators failed to follow procedures in two instances related to draining of the reactor coolant system (RCS). They failed to verify RCS level when it was required. (Prairie Island)

4.1.2.7 PIMs - Design

- Design inadequacies prevented turbine bypass from fast opening at less than 35% power (Cooper);
- During a LOOP, filters for three safety-related deep draft cooling water service pumps could have become clogged, rendering the pumps inoperable. (Prairie Island)

4.1.2.8 PIMS - Inadequate Procedures

- There was a failure to meet technical specification surveillance requirements for position verification on the emergency core cooling system (ECCS) throttle valve. The valve was subsequently found out of its required position (Sequoyah 1&2);
- Licensee implemented an emergency

action level (EAL) change that decreased the effectiveness of the Emergency Plan without approval by the NRC Changes may have resulted in a failure to declare an ALERT even when a significant transient was in progress. (Sequoyah 1 & 2)

4.1.2.9 PIMs - Inadequate Supervision

- In 1999, inspectors noted that the licensee had failed to count two reportable safety system failures in its performance indicator program. (Prairie Island)

4.1.3 Inspection Findings Summary

Inspection Findings Summaries for individual plants were the next information source reviewed. INEEL reviewed these inspection summaries and identified corresponding human performance issues for a sample of three plants - - Indian Point 2, Harris and Oconee1 - - that were applicable to the initiating events and mitigating systems cornerstones. These are presented in Tables F-1, F-2, and F-3 of Appendix F.

The Indian Point 2 plant inspection report identifies 18 errors and failures in work processes, shown in Table F-1. These failures cover operator requalification deficiencies, quality, technical specification violations, procedure inadequacies, and maintenance failures. Design issues and failure to resolve degraded conditions were also noted. Summary inspection findings for the two other plants, Harris and Oconee 1, followed a similar pattern. Findings for these plants are presented in Tables F-2 and F-3, respectively.

Issues identified at Harris included inadvertent safety injection, inaccurate risk assessment for startup transformer, failure to take corrections actions after multiple trips of the emergency services chilled water chiller, and failure to maintain procedures. Also noted were violation of technical specifications due to inoperable ECCS flow path, and operating while having only one charging safety injection pump operable. Oconee 1 human performance problems included inadequate corrective actions on BWT level instrumentation, reactor protection system (RPS) setpoints outside allowable limits, failure to adequately perform valve alignment procedures, failure to follow work control procedures, delaying maintenance, and apparent violations related to emergency feedwater design.

The Safety System Design and Performance Capability procedure directly or indirectly covers such areas as equipment alignment, in-service testing, operator requalification (also reviewed under its own SDP), safety system design and performance capability, fire protection, permanent plant modifications, and maintenance rule implementation. Human performance certainly cuts across all of these functional areas. Tables F-1 through F-3 indicate that a large number of human performance problems were identified through the ROP.

4.1.4 Human Performance Influences and the ROP

Table 4-1 presents an analysis evaluating the ability of the ROP to detect errors determined from operating events (See Appendix B) More general event findings i.e., the presence of latent, multiple, concurrent failures in operations, design, maintenance, and CAPs) have been discussed previously in Section 3 and in NUREG/CR-6753. INEEL plant systems/PRA, human factors/HRA, and operations analysts have evaluated these detailed findings and addressed these findings in terms of three different questions. First, would the findings likely be detectable within the scope of the ROP following current instruction and guidance? Second, would these findings be explicitly considered in contemporary HRA/PRA? Third, were these detailed findings present in multiple operating events?

Inspection of Table 4-1 reveals the following. The ROP is highly likely to detect improper maintenance of safety grade systems and inadequate operator recovery for acknowledged sequences. The ROP is moderately likely to detect the following: failure to follow safe work practices involving

safety systems, design deficiencies, problems in various maintenance and test activities. It is also moderately likely to detect the impact of adverse weather upon staffing levels or ergonomics, any history of false or spurious actuations, and licensee failures to follow industry or NRC notices.

The ROP is less likely to detect the following potential human performance issues: crew knowledge regarding ex-control room activities, presence of latent, dependent failures, improper maintenance of non-safety grade equipment, support system failures contributing to atypical plant response, mismatch between plant procedures and plant conditions, use of informal procedures, influence of distracting conditions on personnel performance, maintainer knowledge deficiencies, and command and control and resource allocation problems.

PRA models consist of event sequences containing a series of basic events. Human error is generally accounted for implicitly in the unavailability values assigned to components and systems. Human error is also considered explicitly in terms of post-initiator human actions. For example, implicit consideration is given to a variety of maintenance practices. It is highly likely that a considerable proportion of errors for risk significant equipment in this area would be detected through the current ROP. The ROP, as evidenced in a number of inspection reports, also does a good job of detecting errors similar to those found in events that are not usually considered in an explicit fashion in PRA. These include: errors in trending of problems, recurrent problems, errors in command and control, and failures in maintenance work practices.

Human performance findings were also examined to determine whether they are typically considered in PRA/HRA. In some instances they may be considered but only in unusual cases or when 2nd generation HRA models are applied. In 11 instances, the error or failure type identified in Column 1 is only considered in emerging or second generation HRA methods such as A Technique for Human Event Analysis (ATHEANA) and others (see Hollnagel 1998, Strater 2000). Six failure types are implicitly considered in risk assessment. These include: design deficiencies, improper maintenance for safety and non-safety grade systems, failures in underlying work processes, adverse weather impact upon staffing levels, and maintenance worker technical knowledge. Only one failure category resulting from error– recovery actions- is routinely considered in an explicit fashion where it is represented as a human failure event or unsafe act.

Six failures including operator technical knowledge regarding ex-control room activities, design deficiencies, latent dependent errors, improper maintenance of non safety grade systems, failures in underlying work processes, and distracting conditions were present in a large number of events. The remainder of the human error present in events was distributed in the following manner. Eight failure categories were present in a moderate number of events and five of these failures were present in a limited number of events. Details are present in Table 4-1

4.1.5 Summary Findings

The working hypothesis for this effort was that the ROP identifies the same human performance issues that were identified through analyses of operating events. This project found this to be the case; the ROP has the potential to identify the same human performance issues contributing to significant operating events. Many of these issues are likely to be contained in "no color findings" in baseline inspection reports, in plant issues matrices (PIMs), in problem identification and resolution inspection findings regarding licensee corrective action programs (CAPs), in the significance determination process (SDP) for operator requalification, and supplemental inspections that evaluate licensee root cause analysis. If implementation of the current maintenance rule was expanded to encompass periodic sampling of maintenance tasks in risk-significant non-safety grade systems, additional human performance issues might be identified. Additionally, event analysis conducted outside of the baseline inspection

process has the potential to identify and characterize human performance issues not covered as part of the ROP.

- **General Finding.** The ROP can detect many of the human performance issues that can impact risk through its baseline inspections process, supplemental inspections, performance indicators, cornerstones, and cross-cutting issues.

- **Risk Informed Inspection Notebooks.** Risk Informed Inspection Notebooks are an important tool for inspectors, ensuring that inspections will be appropriately focused. The worksheets identify shaping factors for the inspectors to use in their assessments involving human performance. These shaping factors are considered in most probabilistic risk assessment (PRA) and human reliability analysis (HRA) analyses.

- **PIMs** PIMs for four pilot plants revealed deficiencies in configuration management, CAPs, engineering test and evaluation, inadequate post maintenance test, inadequate maintenance and actions, operator actions, knowledge and training, procedures and supervision. These are the same types of human performance issues found through operating event analyses.

- **Latent and Active Failures.** Previous work conducted by the INEEL identified a 4:1 ratio of latent to active errors contributing to operating events. The ratio of latent to active errors was 3:1 in ROP pilot and non-pilot inspection reports indicating a similar trend. The ROP does not currently follow a standardized approach to detecting and characterizing these latent factors.

- **Profile of Human Performance in the ROP.** Procedure deficiencies, configuration management deficiencies, and CAP deficiencies represent the majority of human performance issues identified in inspection reports. Operating events contain the same issues, and several others including design and maintenance issues. The findings from this study indicate that the ROP would not detect all of these deficiencies.

- **Relationship of Human Performance Issues in Events to the SDP.** To trigger the SDP, individual or trended human performance should challenge risk important systems. Many of the individual human performance risk-important contributors to operating events would not have triggered the SDP until combined with other human and hardware failures. Such information is not currently available to allow for trending of human performance issues that, by themselves, would fail to trigger the SDP.

For example, during the Comanche Peak (1995) loss of feedwater event, errors in the main feed pump design combined with an inadequate non-safety grade inverter power transfer function and governor valve stem corrosion on two turbine driven auxiliary feedwater (TDAFW) pumps to cause the event. Independent of one another, these errors or failures were insufficient to trigger the SDP.

- **Communications.** Communication factors were influential in events. Currently, other than through emergency preparedness evaluation, and observation of crew cooperation and communication during simulator exercises, the ROP does not directly assess aspects of communication.

Communication factors were influential in events such as: (1) Oconee 2 loss of offsite power (LOOP) (1992); (2) working outside the technical specification limits leading to a spurious reactor scram and turbine generator failure to trip at Riverbend (1994); and (3) inadequate pre-job briefings at Callaway (1992) that did not mention previous spurious trips in the OT-delta-T circuit, which adversely affected work planning, ultimately leading to a reactor trip.

Table 4-1. Types of Human Errors in Events: Frequency and Likelihood of Detection by ROP

Human Error from Event Sources	Frequency of Occurrence in ASP Events***	ROP Likelihood to Detect*	Explicitly Considered in Probabilistic Risk Analysis (PRA)/HRA**
Crew failure to possess knowledge regarding ex-control room activities	H	L	NU
Failures in underlying work processes	H	L	I
Design deficiencies	H	M	I
Presence of latent dependent failures	H	L	NU
Improper maintenance of non-safety grade systems	H	L	I
Distracting conditions	H	L	NU
Improper maintenance of safety grade systems	M	H	I
Failure to respond to industry notices	M	M	NU
Failure to follow safe work processes	M	M	NU
Support systems impact plant control and generate atypical plant response	M	L	NU
Scheduling of conflicting maintenance and test activities	M	M	NU
Informal procedures	M	L	NU
Command and Control and Resource Allocation	M	L/M	NU
Maintainer technical knowledge and command & control	M	L	I
Inadequate Operator recovery for acknowledged sequences	L	H	E
Adverse weather modifies staffing level or ergonomics	L	M	I
Unusual, outside of final safety analysis report (FSAR) context for events	L	L	NU
History of false/spurious automatic actions	L	M	NU
Mismatch between plant procedures and plant conditions	L	L	NU

*Detection Likelihood; H = highly likely, M = moderately likely, L = less likely;

** Consideration in PRA; E = Explicit in PRA, I = Implicit in PRA, NU – not usually considered except with emerging methods such as ATHEANA, CREAM, CAHR, MERMOS or FACE;

*** Failure frequency in events; H= present in a large number of events, M = present in a moderate number of events, L = present in a low or small number of events.

- **Grouping of Human Error Categories.** Statistical analysis of operating event data demonstrated that 60% of operating events can be characterized by four groups of human error categories: (1) design and maintenance, (2) design, maintenance, and operations, (3) design, maintenance, and CAP, and (4) operations, procedures, and CAPs. Many of the human errors involved improper maintenance of non safety-grade systems. Detection of these maintenance factors is unlikely without increased sampling of maintenance activities on safety-grade and non safety-grade systems.

- **Design Issues.** The ROP "design" cornerstone addresses the design issues found in operating events. However, there are two requirements to characterizing these issues. First, the systems with the underlying latent design failure are selected from a group of safety grade systems. Second, once a group of safety grade systems is selected, only a sample of these systems are subject to review. Thus, sampling and selection factors can reduce the likelihood of detecting safety as well as non-safety grade systems with underlying latent failures.

- **Respond to Industry Notices.** Twenty percent of operating events evidenced failures of utilities to respond to industry notices regarding equipment defects or the need for modified work practices. Currently, the means to detect such latent failures is through maintenance rule implementation and the Problem Identification and Resolution review conducted once per year by inspectors.

- **Corrective Action Program and Risk.** Operating event reviews indicate that deficiencies in licensee CAPs contributed to 41% of events. For example, recurrence of circuitry failures, seal failures, safety valve re-seating failures, and repetitive diesel generator failures to start contributed to events. ROP guidance instructs inspectors to consider risk insights and risk importance in selecting corrective action deficiencies for review.

- **Diverse Errors Combine in Events.** Diverse human errors influenced the occurrence or severity of operating events. The mechanisms by which various errors combine to produce failures are neither readily apparent nor easily modeled. These contributors to hardware failures and human failures that impact safety and non safety-grade systems, highlight the role of human performance as a crosscutting issue. Additionally, current HRA screening analysis procedures would potentially discard these smaller latent errors.

- **Training Issues Involving Non-Licensed Operators.** A number of Licensee Event Report (LER) event descriptions include failure by personnel other than licensed operators. The current ROP focus is primarily on licensed operators through the requalification SDP, but there is also a supplemental inspection on training that has broader applicability.

For example, lack of understanding of the relay protection scheme at McGuire Unit 2 (1993) contributed to a LOOP and subsequent plant trip. At Indian Point 2 (1999), inadequate station manager's training resulted in misunderstanding subsequent plant vulnerabilities resulting from partial loss of power. Instrumentation and control (I&C) technicians' requalification training for relays at DC Cook (1995) was inadequate. Unavailability of an inverter qualified electrician at Fort Calhoun Unit 1 (1992) contributed to a loss of heat sink leading to a LOOP event. Work package lineup and technical knowledge deficiencies regarding battery charger operations at Oconee Unit 2 (1992) contributed to a LOOP with failed emergency power.

- **Procedural Inadequacies Contributing to Events.** Thirty-eight percent of LER event descriptions contained evidence of procedural irregularities in design, construction, or procedural compliance.

These deficiencies primarily affected normal, abnormal, and maintenance procedures.

- Currently, procedures are indirectly assessed when work packages are reviewed, under the operator requalification SDP, during use of post-maintenance testing inspection procedures, during evaluation of surveillance testing inspection procedures, during the assessment of personnel performance during non-routine operations, or during corrective action plan review conducted under Problem Identification and Resolution. There are direct assessments of procedures using supplemental inspection for the quality of procedures and, as part of the human factors supplemental inspection, for the use and adherence to procedures.

  - Normal Operating Procedures – Relay bus transfer procedures were inadequate at Oconee (1992); incorrect control switch positions were specified at Sequoyah for Units 1 & 2 (1992); and, lack of cautions in shutdown/cooldown procedures warning of common cause failure (CCF) in letdown storage tank (LDST) instrumentation at Oconee 3 (1997). Inadequate procedures contributed to draining of the reactor coolant system (RCS) during residual heat removal (RHR) operations at Wolf Creek (1994).

  - Abnormal Operating Procedures – Lack of procedures for frazil icing at Wolf Creek (1996) led to a loss of ultimate heat sink; there were no procedures for verifying emergency start of hydro units at Keowee (Oconee 2 1992); and inadequate detail in centrifugal charging pump (CCP) calibration procedures lead to the CCP being operated at full flow excessively at DC Cook (1995). Inadequate maintenance procedures caused a reactor scram and isolation signal during securing of the diesel generators at Oyster Creek (1992).

5. DISCUSSION

5.1 Insights

Recent improvements to the reactor oversight process have made it more objective, reliable and consistent. The ROP has demonstrated the potential to identify risk important human performance issues, including many present in operating events. These changes have been received positively as evidenced through inspector and stakeholder comments in public forums. For example, plant-specific inspection notebooks have the potential to be a valuable aid to inspectors by highlighting important event sequences, identifying risk significant equipment, and characterizing human actions documented in IPEs. Another positive feature of this process is that worksheets accompany these plant specific notebooks.

A recently released summary by the ROP external review group (2001) stated that inspectors were concerned about the possibility of cross cutting areas of human performance, safety conscious work environment, and problem identification and resolution becoming degraded without being detected by the baseline inspection program and performance indicators. They also felt that the current process does not have sufficient criteria, thresholds, and definitions of cross cutting issues, to ensure consistency in handling these issues. The ROP does not provide for additional NRC engagement on cross cutting issues unless they are contributing causes to performance indicators or inspection findings that have been characterized as white or greater. Additionally, some inspectors are also concerned about the lack of a process to handle low-level human performance trends when it appears that NRC actions could prevent the occurrence of a significant performance issue. The sections below discuss insights in this regard. These insights were derived through review of ROP documentation, inspection findings, and analysis of human performance in operating events.

5.1.1 Crosscutting Nature of Human Performance

- Human performance was a major contributor to risk in operating events. Human performance issues in operating events cut across a number of areas - operations, design and design change work practices, maintenance practices and maintenance work control, procedures, design and development process, CAP, and management oversight.

5.1.2 No Color Findings

- In recent stakeholder meetings held in Rockville, Maryland (April 2000), there was discussion regarding eliminating "no color" findings from inspection reports. Eliminating "no color findings" because they are of low risk significance may objectify current practices. However, many human performance insights that individually fail to trigger the SDP, when combined may be useful from a risk-informed perspective. If the practice of reporting these insights is discontinued, the combination of small failures and patterns found in these reports that map to human performance in operating performance will be unavailable in raw form for review.

5.1.3 Latent Failures

- The impact of latent factors, including recurrent utility problems and failure to respond to industry notices of event risk has been established in earlier INEEL research and is presented in NUREG/CR -6753. As currently configured, the ROP most directly detects and documents these factors through one of the following: operator requalification SDP review of knowledge deficiencies, "no color findings in inspection reports,"

review of the licensee CAP backlog, and the inspection procedure for safety system design.

- The ratio of latent to active failures present in operating events was 4:1. In pilot and non-pilot inspection reports, the ratio of latent to active failures was 3:1, indicating a similar trend.

5.1.4 Human Performance Profiling

- The majority of human performance issues identified in inspection reports were from procedure, configuration management, and CAP deficiencies. There was less identification of maintenance as a finding than was the case for operating events.

- When analyzed by error category, 60% of events fell into one of four groups of human error categories: (1) design and maintenance, (2) design, maintenance, and operations, (3) design, maintenance, and corrective action program, and 4) operations, procedures, and corrective action program.

Many of the failures in operator events involved improper maintenance of non-safety grade systems. It is not likely that these maintenance failures would be detected without increased sampling of maintenance activities on safety grade and non-safety grade systems.

5.1.5 Design and CAP Issues

- **Design.** The design issues that are found in operating events are related to the design cornerstone of the ROP. However, there are two impediments to the ROP characterizing these contributions. First, the systems with the underlying latent design failure need to be selected. Second, once selected among a group of potentially risk significant systems, the system needs to be sampled. These two factors combine to increase the difficulty of detecting systems with underlying latent failures.

- **Licensee failure to respond to industry notices.** At least 20% of the events involved failure of a utility to respond to industry notices on equipment defects or the need for new industry practices. Currently, the means to detect this type of latent failure would reside within the Problem Identification and Resolution review, conducted once per year by inspectors.

5.1.6 Significant challenges

- Diverse failures combined in operating events. The mechanisms by which various factors combine appears to be as much a challenge for probabilistic safety analysis (PSA) modelers as it is for inspectors. There is a lack of clear guidance in the ROP for inspectors to integrate multiple, diverse factors to achieve a SDP threshold. Similarly, there is a lack of guidance in PSA on the linkages, (i.e., dependencies) among various human performance influences.

Maintenance failures were significant contributors to operating events. Sensitivity to such failures is important to support identification and characterization of such risk important factors.

5.2 Trends

Human performance crosscutting issues are identified indirectly by performance indicators, and explicitly by baseline inspections. By using safety cornerstones the ROP is more objective than the previous approach that relied upon SALP functional areas and a deterministic approach to evaluation.

In the ROP, certain latent failures in non-safety grade systems without a clear impact upon safety functions may not be fully characterized due to the risk-informed approach to regulation (i.e., only risk-significant failures are to be reported). Even if a deterministic approach were to be taken, it is not known which small latent errors are more likely to combine to help cause or contribute to events. Results from operating events

demonstrated that non-safety grade failures have the potential to affect the context of events and risk.

The trending of low safety significance problems and issues has the potential to indicate declining plant performance. However, developing a metric for combining declines in human performance that may portend significance at a later date may be an area for human performance research.

Event analyses underscore the importance of mechanisms underlying cross-system human factor dependencies. That is, the manner by which smaller failures combine to contribute to risk is not well understood. This issue is also a challenge for the current generation of PRA/HRA.

5.3 Future Considerations

Advances in the field of human reliability assessment include the consideration of errors of commission, enhanced description of context, increasing emphasis on work planning and decision making as they effect risk, recognition of the importance of communication, and the use of work process information in determining the appropriate ways to characterize human performance. These factors are known to be important in operating events. Some of this information is useful in increasing our fundamental understanding of human performance in nuclear power plant settings. Other information has been useful in model building. Still other information has been useful to support measurement and quantification. As knowledge in these areas continues to mature and concepts are incorporated in PRA, it will be possible to gain insights that can support the reactor oversight inspection process.

6. REFERENCES

Gertman, D.I., Hallbert, B.P., Schurman, D.L., & Thompson, C. Management and Organizational Factors Research: The Socio-organizational contribution to risk assessment and the technical evaluation of systems (SOCRATES). In A. Mosleh & R.A. Bari (Eds.), *Proceedings of the 4th International Conference on Probabilistic Safety Assessment and Management PSAM-4.* New York: Springer-Verlag, September 13-1998.

Hollnagel E., *Cognitive Reliability and Error Analysis Method (CREAM)* New York, Elsevier, 1998.

Lanksbury, R.D. *Prairie Island Inspection Reports 50-282/99006 (DRP); 50-306/99006 (DRP).* Washington, DC: U.S. Nuclear Regulatory Commission. Memo from Chief, Reactor Projects Branch 5, to M. Wadley, Northern States Power Co., August 12, 1999.

Nuclear Energy Institute. NEI 99-02 Rev 0, *Regulatory Assessment Performance Indicator Guidelines,* Washington, DC, March 2000.

Reactor Oversight Process Initial Implementation Evaluation Panel (IIEP) Final Report, ADAMs ML011290025, US Nuclear Regulatory Commission, conducted under the Federal Advisory Committee Act, May 10, 2001.

Reason, J. *Human Error.* Cambridge, U.K: Cambridge University Press, 1990.

Sträter, O. Evaluation of Human Reliability on the Basis of Operational Experience. GRS-170. Koln, Germany: German Institute for Reactor Safety (GRS). 2000.

U.S. Nuclear Regulatory Commission. MC 0305, *Operating Reactor Assessment Program.* Washington, D.C.

U.S. Nuclear Regulatory Commission. MC 0609, *Significance Determination Process,* Washington, DC. http://www.nrc.gov/NRR/OVERSIGHT/ROP/documents.html,February, 2001

U.S. Nuclear Regulatory Commission. MC 0610, *Inspection Reports (Draft 4/24/00).* Washington, DC. http://www.nrc.gov/NRR/OVERSIGHT/ROP/documents.html, 2000

U.S. Nuclear Regulatory Commission. MC 02515A, *Risk-Informed Baseline Inspection Program.* Washington, DC. http://www.nrc.gov/NRR/OVERSIGHT/ROP/documents.html, March 6, 2001.

U.S. Nuclear Regulatory Commission. Inspection Procedure 71841, *Supplemental Inspection for Human Performance.* Washington, DC. October 2000 (draft under review).

U.S. Nuclear Regulatory Commission. NUREG-0700, Rev. 1. *Human System Interface Design Review Guidelines.* Washington, DC. June 1996.

U.S. Nuclear Regulatory Commission. NUREG/CR-6753 *Review of Findings for Human Performance Contribution to Risk in Operating Events,* Gertman, D., et. al., Idaho National Engineering and Environmental Laboratory, September 2001

U.S. Nuclear Regulatory Commission. NUREG-1649. *Reactor Oversight Process.* Washington, DC, 1999.

U.S. Nuclear Regulatory Commission. Regulatory Guide 1.174 *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis*, Washington D.C. July 1998.

U.S. Nuclear Regulatory Commission. SECY-99-007A. *Recommendations for Reactor Oversight Process Improvements.* Washington, DC. http://www.nrc.gov/NRR/OVERSIGHT/ROP/documents.html, 1999.

U.S. Nuclear Regulatory Commission. SECY-00-049. *Results of the Revised Reactor Oversight Process Pilot Program.* Washington, DC. http://www.nrc.gov/NRR/OVERSIGHT/ROP/documents.html, 2000.

U.S. Nuclear Regulatory Commission. SECY-090-337. *Procedural Adherence Requirements.* Washington. DC, 1990.

U.S. Nuclear Regulatory Commission. NUREG-1021. Rev. 8. *Operator Licensing Standards for Power Reactors.* Washington, DC, 1998.

Inspection Manual Chapter 2515A. Appendix A. *Risk-Informed Baseline Inspection Program,* April 2000.

APPENDIX A

CORNERSTONES AND PERFORMANCE INDICATORS

A1. Initiating Events Cornerstone

The objective of this cornerstone is to limit the frequency of those events that upset plant stability and challenge critical safety functions, during shutdown as well as power operations. If not properly mitigated, and if multiple barriers are breached, a reactor accident could result which might compromise public health and safety. Licensees can reduce the likelihood of a reactor accident by maintaining a low frequency of these initiating events. Such events include reactor trips (scrams) due to turbine trips, loss of feedwater, loss of off-site power, and other reactor transients.

There are three performance indicators in this cornerstone:

- Unplanned Scrams - The number of unplanned scrams during the previous four quarters, both manual and automatic, while critical per 7,000 hours. The scram rate is calculated per 7,000 critical hours because that value is representative of the critical hours of operation in a year for a typical plant.

- Scrams with Loss of Normal Heat Removal - The number of unplanned scrams while critical, both manual and automatic, during the previous 12 quarters that also involved a loss of the normal heat removal path through the main condenser.

- Unplanned Power Changes - The number of unplanned changes in reactor power of greater than 20% full-power, per 7,000 hours of critical operation excluding manual and automatic scrams.

A2. Mitigating Systems Cornerstone

The objective of this cornerstone is to monitor the availability, reliability, and capability of systems that mitigate the effects of initiating events to prevent core damage. Licensees reduce the likelihood of reactor accidents by maintaining the availability and reliability of mitigating systems. Mitigating systems include those systems associated with safety injection, decay heat removal, and their support systems, such as emergency AC power. This cornerstone includes mitigating systems that respond to both operating and shutdown events.

There are five indicators in this cornerstone:

- Emergency AC Power System - Safety System Unavailability - The average of the individual train unavailabilities. Train unavailability is the ratio of the hours the train is unavailable to the number of hours the train is required to be able to perform its intended safety function.

- High Pressure Injection System -Safety System Unavailability - The average of the individual train unavailabilities.

- BWR Heat Removal System/PWR Auxiliary Feedwater System -Safety System Unavailability - The average of the individual train unavailabilities.

- Residual Heat Removal System -Safety System Unavailability - The average of the individual train unavailabilities.

- Safety System Functional Failures - The number of events or conditions that alone prevented, or could have prevented, the fulfillment of the safety function of structures or systems in the previous four quarters.

A3. Barrier Integrity Cornerstone

The objective of this cornerstone is to provide reasonable assurance that the physical design barriers protect the public from radio nuclide releases caused by accidents. Licensees can reduce the effects of reactor accidents if they do occur by maintaining the integrity of the barriers. The barriers are the fuel cladding, reactor coolant system boundary, and the containment.

There are two indicators in this cornerstone:

- Reactor Coolant System (RCS) Activity - The maximum monthly RCS activity in micro-Curies per gram (μCi/gm) dose equivalent Iodine-131 per the technical specifications, expressed as a percentage of the technical specification limit.

- Reactor Coolant System (RCS) Leakage - The maximum RCS Identified Leakage in gallons per minute each month as defined in Technical Specifications, expressed as a percentage of the technical specification limit.

A4. Emergency Preparedness Cornerstone

The objective of this cornerstone is to ensure that licensees are capable of implementing adequate measures to protect public health and safety during a radiological emergency. Licensees provide reasonable assurance that their emergency preparedness program is effective through drills and exercises, participation in actual events, and testing of the Alert and Notification System (ANS). This cornerstone does not include the off-site actions, which are covered by FEMA.

There are three indicators in this cornerstone:

- Drill/Exercise Performance - The percentage of all drill, exercise, and actual opportunities that were performed accurately and in a timely manner during the previous eight quarters.

- Emergency Response Organization (ERO) Drill Participation - The percentage of key ERO members that have participated in a drill, exercise, or actual event during the previous eight quarters, as measured on the last calendar day of the quarter.

- Alert and Notification System Reliability - The percentage of ANS sirens that are capable of performing their function, as measured by periodic siren testing, in the previous 12 months. Periodic tests are the regularly scheduled tests that are conducted to actually test the ability of the sirens to perform their function (e.g., silent, growl, and siren sound test).

A5. Occupational Radiation Safety Cornerstone

The objective of this cornerstone is to ensure adequate protection of worker health and safety from exposure to radiation from radioactive material during routine civilian nuclear reactor operation. This exposure could come from poorly controlled or uncontrolled radiation areas or radioactive material that unnecessarily exposes workers. Licensees can maintain occupational worker protection by meeting applicable regulatory limits and ALARA guidelines.

There is one indicator in this cornerstone:

- Occupational Exposure Control Effectiveness - The performance indicator for this cornerstone is the sum of the following;
  - Technical specification high radiation area occurrences
  - Very high radiation area occurrences
  - Unintended exposure occurrences

A6. Public Radiation Safety Cornerstone

The objective of this cornerstone is to ensure adequate protection of public health and safety from exposure to radioactive material released into the public domain as a result of routine civilian nuclear reactor operations. These releases include routine gaseous and liquid radioactive effluent discharges, the inadvertent

release of solid contaminated materials, and the offsite transport of radioactive materials and wastes. Licensees can maintain public protection by meeting the applicable regulatory limits and ALARA guidelines.

There is one indicator in this cornerstone:

- Radiological Effluent Technical Specifications/Offsite Dose Calculation Manual (RETS/ODCM). Radiological effluent release occurrence per reactor unit that exceed the values listed below:

  - Liquid Effluents
    - Whole Body - 1.5 mrem/qtr
    - Organ - 5 mrem/qtr
  - Gaseous Effluents
    - Gamma Dose - 5 mrads/qtr
    - Beta Dose - 10 mrads/qtr
    - Organ Doses from I-131, I-133, H-3 & Particulates - 7.5 mrems/qtr

A7. Physical Protection Cornerstone

The objective of this cornerstone is to provide assurance that the safeguards program will function to protect against the design basis threat of radiological sabotage. The threat could come from either external or internal sources.

Licensees can maintain adequate protection against threats through an effective security program that relies on a defense in depth approach.

There are three indicators in this cornerstone:

- Protected Area (PA) Equipment - PA Security equipment performance is measured by an index that compares the amount of time closed circuit television cameras (CCTVs) and intrusion detection system (IDS) are unavailable, as measured by compensatory hours, to the total hours in the period. A normalization factor is used to take into account site variability in the size and complexity of the systems.

  - Personnel Screening Program - The number of reportable failures to properly implement the regulatory requirements of 10 CFR 73.56 and 73.57.
  - Fitness-For-Duty (FFD)/Personnel Reliability Program - The number of reportable failures to properly implement the requirements of 10 CFR Part 26.

Assessment Process. Frequency. There are four levels of review of licensee performance: continuous, quarterly, semiannual, and annual. The action decision model is part of the assessment process and includes an action matrix. Actions are categorized into four areas: management meeting, licensee action, NRC inspection, and regulatory action. They are graded across five ranges of licensee performance.

One concern that we would have is that as performance indicators become more numerous would inspection be reduced and more paper work based so as not to increase the burden on utilities. For example, it may be difficult to determine human performance issues with a cumulative effect, given that less inspections or less frequent inspections are conducted. There is an implicit assumption that if the utility has to perform additional reporting of indicators that inspections would be reduced for the risk reduction gained by refining the performance indicator set.
Severe accident management is an industry initiative and not a requirement. Therefore, it is not inspected under the program.

APPENDIX B

DETAILED PERFORMANCE FINDINGS

B1. Operations

B1.1 Command and Control including Resource Allocation

Beaver Valley 1, 334-93-013,

- While verifying auxiliary contact alignment, maintenance personnel caused inadvertent actuation of an under frequency electrical breaker separation scheme causing a loss of electrical load, LOOP, and a reactor trip. Operations department personnel were not included in switchyard work planning.

Hatch Unit 1, 372-00-002,

- 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).

Indian Point 2, 247-99-015,

- Recovery actions were poorly coordinated following a reactor trip from a spurious signal.
- Station supervision failed to ensure that the plant staff responded to assist operators in mitigating the degraded plant conditions.
- Station supervision failed to establish expectations that recovery from the degraded plant conditions had priority over preparations for shutdown work activities.
- Following a spurious reactor trip, incorrect electrical lineups and electrical equipment failure resulted in loss of vital AC, vital DC, and instrument AC power. Technical support failed to minimize time in degraded conditions with significant high-risk failures, taking excessive time for electrical measurements.

McGuire 2, 370-93-008,

- The shift supervisor failed to function as the senior operator in charge of the event following a turbine and reactor trip from a failed insulator. The supervisor acted as the EOP reader for approximately 15 minutes, reducing his ability to oversee the event.
- Operators failed to complete the licensee notification procedure and correspondingly notify the NRC within the time allotted. This resulted in inaccurate and incomplete reporting of the event.

Oconee 2, 270-92-004,

- Keowee (KH) Unit 1 hydroelectric generating station personnel took inappropriate actions without concurrence or direction from the Oconee control room. These actions had an impact on the Oconee emergency power that could have interfered with the safety function of emergency power. The level and significance of problems at KH were not fully understood or communicated by Oconee.

Sequoyah 1&2, 327-92-027,

- The shift supervision failed to call in a replacement operator for an absentee operator. This resulted in insufficient staffing to respond to a dual plant trip and a lack of understanding of the effect of two simultaneous trip evolutions. The crew subsequently allowed an excessive rate of cooldown rate in the reactor coolant system.

Wolf Creek, 482-96-001,

- Control room staff performed an unfamiliar evolution without using a procedure or second operator verification of the evolution lineup. The operators missed several opportunities to correct system misalignments due to poor communications and poor self-checking techniques.

Oconee 3, 287-97-003,

- An high pressure injection (HPI) pump was damaged during a plant cooldown when operators failed to verify letdown storage tank level. Operators pumped the tank down for 2 hours without independent observation of control room activities and indications by an independent operator such as an shift technical advisor or senior reactor operator (SRO).

Salem 1, 272-94-007,

- Management guidance was lacking for control room operator activities during a plant power reduction caused by river grass intrusion at the intake structure.
- A rapid downpower evolution with multiple reactivity changes was poorly controlled. The nuclear shift supervisor (NSS) gave the reactor operator vague directions to pull rods to restore T_{ave}. Requests for additional information by the RO were not addressed.
- A reactor operator was incorrectly directed to leave the reactor console controls while reactivity was not stable.

Wolf Creek, 482-94-013,

- While shut down, the plant experienced an unexpected decrease in reactor coolant level due to operator error. Shift supervision failed to inform the crew of on-going evolutions and lacked understanding of the effect of performing simultaneous evolutions.

Failure to Follow Safe Work Practice

Oconee 2, 270-92-004,

- A work package incorrectly placed a battery charger in a lineup to supply power without the battery connected. Doing so was a poor practice for battery chargers and was outside the design capabilities of the equipment.

Inadequate Knowledge or Training

Hatch Unit 1, 372-00-002,

- Operators failed to fully recognize the impact of plant conditions on control room indications.
- Reactor core isolation cooling (RCIC) restart training was inadequate.

Indian Point 2, 247-99-015, AIT-247-99-08,

- Vital AC, vital DC, and instrument AC power were lost following a spurious reactor trip due to incorrect electrical lineups and electrical equipment failure. Station managers did not anticipate the vulnerabilities caused by the loss of power.
- Lack of Technical Specification knowledge caused late entry into a TS limiting conditions for operation (LCO).
- Knowledge of the regulatory requirements and safety design basis for maintaining the transformer load tap changer in automatic was lacking.

McGuire 2, 370-93-008,

- Undue reliance was placed on a non-safety related turbine runback feature during electrical power disturbances. The licensee did not appear to understand the switchyard relay protection scheme.
- Operators did not recall training that emphasized a modification to some steam drain valves that changed their fail-safe position from open to closed on loss of power. Rather, relying on past experience and incorrect simulator response, they incorrectly jumpered these valves closed which actually opened them.

Oconee 2, 270-92-004,

- A DC control power problem with the 230-kV switchyard caused a bus lockout and switchyard isolation. Unit 1 generator separated from the grid, oversped, and locked out. operators demonstrated lack of knowledge in responding to their control room annunciation and abnormal conditions, which could have interfered with the emergency power safety function.
- Live bus transfer training and the governing procedure were inadequate.
- Oconee control room personnel were not aware of some electrical system details and interlock features. This resulted in an

inadvertent loss of both units during the recovery phase.

Riverbend, 458-94-023,

- The turbine generator failed to trip as expected during a spurious reactor scram. Subsequent investigation of generator trip actions by operators revealed that operator knowledge and understanding of main turbine generator operation and fast/slow transfer of station loads was not clear.

Sequoyah 1&2, 327-92-027,

- Operators failed to understand the impact that system lineups for ongoing evolutions would have during a dual unit trip. This allowed the charging pumps to operate without a suction source and prevented other equipment from responding as required for plant conditions.

Wolf Creek, 482-96-001,

- A reactor trip was caused by loss of level in the circulating water and essential service water system (ESWS) suction bays due to icing conditions and freezing of the traveling screens. Operator and engineering knowledge was lacking concerning the conditions that cause Frazil icing and its effects.

Callaway, 483-92-011,

- All MCB annunciators became inoperable when all field contact power supply fuses blew during a failed power supply replacement. With more than half of the MCB annunciators lit, licensed operators incorrectly believed that the unlit annunciators were operable and failed to declare an ALERT as required. Personnel had inadequate knowledge of the annunciator system functions during a loss of power.

Catawba 2, 413-93-002,

- The nuclear service water pump discharge valves failed to open during a pump start. Operators did not understand policy guidance and action statements regarding required surveillances of diesel generators when required by technical specification 3.0.3.

Fort Calhoun, 285-92-023,

- Instrumentation power was lost when a breaker opened while returning an inverter to service following repairs. Diagnosis was hampered by malfunctions in computer displays for containment temperature and RCS subcooling parameters. There was inadequate training for degraded computer operations.
- An inverter-qualified electrician who may have known about missing jumpers in the repaired inverter was not available, which contributed to the breaker trip.

Oconee 3, 287-97-003,

- Operators failed to fully diagnose the cause for an automatic pump start and inappropriately returned the pump to standby. They subsequently failed to diagnose a cavitating HPI pump, which contributed to additional HPI pump damage.

Oyster Creek, 219-92-005,

- The improper securing of a diesel generator caused a reactor scram and isolation. The operator was monitoring the incorrect voltage meter.

Salem 1, 272-94-007,

- While rapidly reducing power in order to take the turbine off line, operators caused a reactor trip and automatic safety injection. They were unaware of the reactor power trip function on low-power, high flux conditions.
- Post event analysis for the trip, which resulted in the pressurizer power operated relief valves (PORVs) opening more than 300 times to prevent RCS overpressure, found operator knowledge of yellow path recovery procedures weak.

Incorrect operator action/inaction

Haddam Neck, 213-93-006/007, AIT 93-080,

- While conducting breaker trip logic testing

during shutdown, a total LOOP occurred due to a wiring error. An operator failed to identify the failure based on earlier abnormal indications of voltage. Control room operators failed to reset lock-in relays when restoring from a SI actuation caused by the loss of power.

- The air receiver for the PORVs decayed faster than allowed by TS. Early detection and correction of the problem was prevented by an improper valve lineup.

Hatch Unit 1, 372-00-002,

- Operators failed observe automatic flow demand before transferring HPCI control from manual back to automatic.

McGuire 2, 37093008,

- During a turbine trip and reactor trip caused by a failed electrical insulator, excessive time taken to read EOP fold-out pages delayed the implementation of procedural steps to isolate MSIVs prior to a safety injection signal. Subsequent actions were taken that opened isolated MSIV drain lines without procedural guidance or use of reference material.

Sequoyah 1&2, 327-92-027,

- During a dual unit trip, operators failed to read and perform the correct procedure. Equipment control switches were in the wrong position preventing required automatic actions. Operators failed to manually perform those actions.

Wolf Creek, 482-96-001,

- A reactor trip resulted from loss of level in the circulating water and ESWS suction bays due to icing conditions and freezing of the traveling screens. Equipment was declared operable without adequate evaluation or determination of root cause. Control room staff missed several opportunities to identify and/or correct system misalignments.

Oconee 3, 287-97-003

- Operators lacked sensitivity to the plant situation. Numerous concurrent duties diverted attention from monitoring plant parameters. Operators failed to act on training and experience, relying on alarms to alert them to unstable conditions.
- Operators failed to fully diagnose the cause for an automatic pump start and inappropriately returned the pump to standby. The operators subsequently failed to diagnose a cavitating HPI pump based on the available indications, contributing to additional HPI pump damage. Control room activities were not independently observed.

Dresden 3, 249-96-004,

- While feedwater regulating valve A (FRV-A) was out of service because of a steam leak, FRV-B failed causing a low reactor water level, scram, and containment isolation. A lack of understanding of defense in depth relationships and risk basis allowed operations in unstable conditions.

Communications

Indian Point 2, 247-99-015/008,

- Work control personnel were not notified of previous spurious trips in the OT-ΔT circuit, which adversely affected work planning. This ultimately led to a reactor trip.
- The calculated daily risk factor was not communicated to senior management, preventing its use to expedite recovery actions and equipment repairs.

Oconee 2, 270-92-004,

- A DC control power problem with the 230-kV switchyard caused a bus lockout and switchyard isolation. Unit 1 separated from the grid, oversped and locked out. Loss of phone communications contributed to response delays. Keowee annunciator and computer alarm printers were lost, preventing system feedback and complicating plant conditions.

Riverbend, 458-94-023,

- During a spurious reactor scram, the turbine generator failed to trip as expected.

Operator communications within the operating crew and outside departments were weak, resulting in operation outside EOP limits and missed technical specification required surveillances.

Sequoyah 1&2, 327-92-027,

- An internal fault in a newly installed switchyard breaker caused a dual unit trip. Inadequate communications existed between work organizations responsible for assessing risks associated with new breaker installation and testing.

St. Lucie 1, 335-97-011,

- Obsolete engineered safety features actuation system (ESFAS) bistables replacement and a lowered setpoint caused a non-conservative setpoint value for ECCS actions. This resulted from ineffective communications between departments associated with the set point change.

Wolf Creek, 482-96-001,

- Engineering incorrectly issued a note that active Frazil ice formation on the trash racks and traveling screen was not a credible event because the pump house was normally heated.

Callaway, 483-92-011,

- All MCB annunciators became inoperable when all field contact power supply fuses blew during a failed power supply replacement. Plant staff failed to conduct a pre-job briefing between the operating crew, the technicians, the planner, and the engineer performing the work. Operations personnel were not informed that all four field contact power supply fuses were blown.

Calvert Cliffs, 318-94-001,

- A reactor trip occurred during installation of 13.8 kV voltage regulators when an electrical protective relay inadvertently actuated causing the loss of power to two non-vital and one vital safety bus. Project team members and the control room failed to communicate adequately. Imprecise terminology was used in project documents and verbal communications.

Salem 1, 272-94-007,

- A rapid downpower evolution in response to river grass intrusion at the intake structure was poorly controlled. The NSS gave the reactor operator vague directions to pull rods to restore T_{ave}. Operators were unaware of the low-power, high flux reactor trip function and caused a reactor trip and automatic safety injection.
- Continual communication from the SRO, whose back was to the control room, added to the general confusion, operator workload, and interfered with time sensitive tasks.

B2. Design and Design Change Work Practices

Design Deficiencies

ANO1, 313-96-005,

- After loss of one main feed pump (MFP) due to an electrical fault, the remaining MFP was lost due to inadequate design of the feedwater control system. The previous design review failed to consider feedwater control during transient conditions.
- Design problems with Safety Parameter Display System temperature sensors required operators to perform manual calculations on the steam generator tube-to-shell differential temperature.

ANO2, 368-95-001

- The design review for replacing electro-hydraulic emergency feedwater valves with motor operated valves (MOVs) failed to consider the voltage decay time following a main generator trip. This invalidated the assumption that the AC powered valves would remain "as-is" on loss of power.

Beaver Valley 1, 334-93-013

- An under-frequency separation scheme in the switchyard inadvertently actuated during a maintenance activity. The design process failed to update the switchyard trip system based on electrical plant loading.

Comanche Peak, 445-95-003/005

- During slave relay testing, an inverter inappropriately transferred from normal to alternate power causing a loss of power to auxiliary relays. This caused a low feedwater pump oil pressure signal that ultimately tripped all condensate and feed system pumps. The transient protection for the inverter was improperly designed, allowing transfer to a de-energized bus.

Oconee 1,2,3, 269-92-018

- A deficient design lead to the failure to power the trip relays for condensate pumps from multiple power sources, allowing a single failure to cause a loss of feedwater and plant trip.
- Subsequent to the trip, the turbine-driven auxiliary feedwater pump tripped on overspeed. The design improperly used a non-Inconel valve stem that corroded and caused binding, preventing proper speed control.

Hatch, 321-00-002

- Operators opened an excessive number of Safety Relief Valves (SRV) prior to receiving an "open" indication when using the SRVs to reduce reactor pressure following a Scram and MSIV isolation. The SRV open tail-pipe pressure switches failed to actuate. A deficient design prevented an "open" indication when passing a steam/water mixture rather than just steam.

La Salle 1, 373-93-015)

- Moisture accumulation in the electrical bus duct caused the loss of the station auxiliary transformer and a reactor scram. The design failed to allow for proper drainage of accumulated moisture.

McGuire 2 370-93-008,

- The turbine failed to runback as expected during a transient from loss of an electrical bus. The runback design relied on a non-safety related feature and failed to reflect the existing switchyard relay protection scheme. There was no testing program for the runback feature.

Oconee 1,2,3, 269-92-018,

- During testing of emergency power supply output breakers, one of breakers could not be closed. The system design failed to consider operation with minimum values for input DC voltages.
- The interaction between low DC voltage and time available for energizing closing coil was not considered in the breaker equipment design.

Oconee 2, 270-92-004,

- A DC control power problem with the 230-kV switchyard caused a bus lockout and switchyard isolation. The battery charger utilized a circuit design containing a defective Zener diode for the application.
- Several design deficiencies in the Kewowee auxiliary load center automatic transfer circuitry lead to loss of the telephone system and alarm annunciation indications.
- A complex and atypical electrical design for the emergency power systems and interacting systems contributed to problems operating these systems.

Riverbend 458-94-023,

- Rosemont transmitters caused a false high water level condition and a reactor scram without any control room indication of reactor water level problems. These Rosemount transmitters had known deficiencies and required special dampening which other maintenance processes negated.

Robinson 261-92-017/013/018,

- The Startup transformer protective circuitry junction box contained water that caused a short and reactor trip. The junction box design, fastener use, and box orientation failed to allow drainage of moisture.
- Foreign material blockage in the minimum flow recirculation line caused loss of both safety injection pumps and a plant shutdown. The design of the SI recirculation pump failed to include

strainers that would have prevented plugging.

Seabrook 443-96-003,

- Personnel observed the turbine driven auxiliary feed pump outboard mechanical seal emitting sparks during a surveillance test. The last seal replacement omitted the use of a dial indicator that was required by the design of seal, which was a non-standard maintenance practice that was omitted from the seal replacement procedure.

Wolf Creek 482-96-001,

- Icing conditions and freezing of the traveling screens caused a loss of level in the circulating water and ESWS suction bays and a reactor trip. The design of warming lines and the design calculation for determining the required flow failed to prevent Frazil icing.

Byron 1, 454-96-007,

- Improper design of the weld on top of the channel and degraded caulk on the bus duct allowed water to enter between an insulator and bus duct causing a trip of the Unit station auxiliary transformer, loss of off-site power, and a reactor trip.

Catawba 2, 414-96-001,

- Inadequate design of bus ducting and resistor bushings allowed moisture intrusion and corrosion causing a phase-to-phase ground fault, LOOP, and reactor trip.

Fort Calhoun, 285-92-023,

- Following a reactor trip from high pressure, a pressurizer code safety valve lifted, closed, lifted again at a pressure lower than the setpoint, and then remained partially open. The safety valve could not tolerate vibrations from liquid in the instrument loop seal because of a poor design. This caused damage to the valve internals that prevented the valve from reseating properly and allowed the setpoint adjustment bolt, which had no locking device, to back out.
- Inadequate control room indications prevented identification of the safety valve failing to reseat.
- The electrical system design precluded post maintenance testing after an inverter board replacement without placing the inverter in service.

Oconee 3, 287-97-003,

- Both letdown storage tank (LDST) level instruments falsely indicated a constant level while actual level dropped to the point where the HPI pump in use was damaged. The poorly designed level instruments used a single reference leg for both channels of LDST instrumentation.

Quad Cities 265-93-010,

- Under voltage testing revealed that the start logic for the cooling water pump for the ½ Diesel Generator prevented automatic starting of the pump under certain conditions. This logic design deficiency existed on both electrical power sources for the pump from the original design.

Turkey Point, 250-92-001,

- The design for seismic qualification of switchgear failed to consider the required normally racked down breaker positions that threatened subsequent operability of the switchgear. The licensing design basis also failed to address the seismic qualification of individual breakers.

Design Change Testing

ANO2, 368-95-001,

- The failure of one train of DC power could also render the other train of emergency feedwater inoperable. Field testing for a design change to replace electro-hydraulic valves with MOVs was inadequate.

ANO1, 313-96-005,

- Operating with less than comprehensive testing of the new digital feedwater control system in the presence of system noise lead to failure on demand, loss of feedwater, and a reactor trip on high pressure.

Oconee 1,2,3, 269-92-018,

- During testing of the emergency generators, one of the output breakers could not be closed. A previous modification to the breaker control circuit and replaced components were not tested under all operating demand conditions.

St Lucie, 335-97-011,

- A loop scaling change for the refueling water tank level indication was made in 1993 without the bistable setpoint correspondingly changed, which could have prevented performance of a safety function. The design change testing process was inadequate and lacked cross checking for bistable sepoints.

Callaway, 483-92-011,

- During restoration of an annunciator field contact power supply failed and was replaced, all field contact power supply fuses blew causing all MCB annunciators to become inoperable. The field power supply replacement failed to specify a retest. The actual testing performed by the I&C technician failed to reveal that the logic power supply fuses were blown.

Calvert Cliffs 2, 318-94-001,

- During installation of 13.8 kV voltage regulators, an electrical protective relay inadvertently actuated causing the loss of power to two non vital and one vital safety bus and a reactor trip. The modification process failed to require integrated testing with the work.

Fort Calhoun, 285-92-023,

- Changing the electro-hydraulic control system (EHC) power supply to a different source failed to correct the problem that it was intended to. Inadequate design change testing for the EHC power source change failed to detect the problem, which ultimately caused a turbine and reactor trip.

Inadequate Engineering Evaluation

ANO2, 368-95-001

- The design review process for the replacement of electro-hydraulic emergency feedwater isolation valves with motor operator valves failed to discover that, during loss of certain power sources, these AC valves do not fail "as is."

Haddam Neck, 213-93-006/007

- Erratic output and abnormal generator indications during a surveillance test required the premature shutdown of an Emergency Diesel Generator. The long-term capabilities of support equipment were not considered. The engineering analysis failed to consider the effect of aging plant components in environments with inadequate cooling.
- The PORVs air receiver pressure decayed faster than allowed. An improper valve lineup intended to monitor moisture content in air system contributed to the inability to detect the malfunction prior to failure.

Indian Point 2, 247-99-015

- The engineering analysis for an EDG load sequencing change failed to consider the blackout loading sequence. The relay tolerances permitted loading multiple pump motors onto the EDG bus at one time.

Limerick 1, 352-95-008

- Steam erosion from pilot valve seat leakage caused an SRV to unexpectedly opened and force a plant shutdown and cooldown.
- Engineering review of the previous valve test results failed to predict and prevent the SRV failure.

Millstone 2, 336-95-002

- The engineering evaluation of valve susceptibility to pressure locking and thermal binding failed to identify a common mode failure that would prevent entry into the containment sump recirculation mode.

Oconee 2, 270-97-001

- An RCS leak caused by a crack on the HPI

to RCS cold leg nozzle sleeve forced a reactor shutdown and cooldown. Ultrasonic testing designed to detect such potential cracks was inadequate.

- The effect of thermal stress on nozzles was not adequate considered in the engineering review, which was not outwardly focused to incorporate industry findings of similar problems.

River Bend 458-94-023,

- Rosemont transmitters caused a false high water level condition and reactor scram without any control room indication of reactor water level problems. The transmitters contained a known deficiency that required special dampening. Other maintenance processes negate the transmitter dampening due to inadequate engineering evaluation.

Wolf Creek, 482-96-001,

- Icing conditions and freezing of the traveling screens caused a loss of level in the circulating water and ESWS suction bays and reactor trip. The enclosure and heating of the emergency service water pump house led to an inadequate engineering evaluation that falsely concluded that Frazil icing could not occur.
- Equipment was declared operable without adequate engineering evaluation or determination of root cause for the failure.

Calvert Cliffs 2, 318-94-001,

- During installation of 13.8 kV voltage regulators, the inadvertently actuation of an electrical protective relay caused the loss of power to two non vital and one vital safety bus and resulted in a reactor trip. Engineering design evaluation of the equipment response during various stages of installation was inadequate.

Catawba 1, 413-93-002

- Incorrect sizing calculations for the unseating and dynamic torque loads under flow and pressure conditions caused the nuclear service water pump discharge valves to fail open during a pump start.
- Engineering inadequately evaluated the effects of valve degradation due to time and wear in determining valve size requirements.

Fort Calhoun, 285-92-023

- Changing the EHC power supply to a different source failed to correct a problem as intended. An inadequate engineering evaluation for the safety valve system design failed to correctly determine the root cause.

South Texas 1, 93-005/007

- A lack of parts forced the licensee to return the turbine driven auxiliary feedwater pump to service with disk and stem steam cuts. The turbine tripped on overspeed during subsequent testing. The engineering evaluation failed to recognize the adverse effects of water accumulation in the TDAFW pump governor valve and turbine casing from leakage through the trip/throttle valve.

Ineffective Abnormal Conditions

Fort Calhoun 285-92-023

- Following a reactor trip from high pressure, a pressurizer code safety valve lifted at a lower pressure than the setpoint and remained partially open. Ineffective operator indications failed to alert control room operators of the safety valve failure to reseat.

Configuration Management

Haddam Neck, 213-93-006/007,

- An motor control center (MCC) was lost when an Automatic Bus Transfer device failed to operate curing surveillance testing of safety injection logic with a partial loss of power. The direct cause was a breaker wiring error that originated from erroneous information in the breaker manual due to inadequate vendor manual configuration control.

Indian Point 2, 247-99-015,

- Incorrect electrical lineups and electrical

equipment failure caused a loss of vital AC, vital DC, and instrument AC power following a spurious reactor. The licensee failed to maintain the station auxiliary load tap changer in the automatic position as required by the licensing bases.

- The 23 EDG output breaker over current set point was not adequately controlled due to inadequate test methodology.
- The degraded voltage relay reset values for the 480 buses were not controlled.

McGuire 2, 370-93-008,

- During a turbine trip and reactor trip caused by a failed electrical insulator, control room drawings and instrument details failed to clearly and unambiguously identify modifications. This could have led to confusion and delay.
- The main turbine failed to runback as expected during a loss of electrical bus transient. A lack of testing for the turbine runback feature resulted in the failure to identify potential design and configuration problems.

St Lucie 1, 335-97-011,

- A 1993 loop scaling change for the refueling water tank level indication without a corresponding bistable setpoint change could have prevented performance of a safety function. An inadequate design engineering process for set point and loop scaling process lacked cross checking for bistable sepoints. Configuration control during instrumentation changes was inadequate.

Catawba, 413-93-002,

- The nuclear service water pump discharge valves failed to open during a pump start due to incorrect torque switch settings. Inadequate labeling of torque switch settings within the MOVs led to the error.

Fort Calhoun, 285-92-023,

- Following a reactor trip from high pressure, a pressurizer code safety valve lifted at a lower pressure than the setpoint and remained partially open. Inadequate technical manual configuration control led to incorrect torque requirements for the SRV setpoint adjusting bolt locknut.

Quad Cities, 265-93-010,

- Undervoltage testing revealed original design problems with the ½ Diesel Generator cooling water pump start logic that prevented automatic starting of the pump under certain conditions. This same logic design deficiency affected both electrical power sources for the pump.
- Incorrect or inadequate labeling and lack of internal breaker logic information on some drawings significantly hindered the detection of the design deficiency over the years.

B3. Maintenance Practices and Maintenance Work Control

Work Package Development and QA

Commanche Peak, 445-95-003,

- During slave relay testing, an inverter inappropriately transferred from normal to alternate power causing loss of power to auxiliary relays. The result was a low feedwater pump oil pressure signal that ultimately tripped all condensate and feed system pumps. Failure to calibrate the static switch logic sense PCB and the analog PCB impaired the inverter's ability to properly respond to transients and resulted in the transfer to a deenergized source.

Dresden 3, 249-96-004,

- Stem and disc separation occurred in a FWRV after inadequate QA of the work package completion allowed a "Not Required" entry and a radial off-set outside of the OEM's recommendation.

Oconee 1,2,3, 269-92-018,

- During testing of the emergency generators, one of the output breakers could not be closed. The work package incorrectly implemented a modification to the anti-pumping circuitry.

Oconee 2, 270-92-004,

- A DC control power problem with the 230-kV switchyard caused a bus lockout and switchyard isolation. Use of a switchgear DC battery charger as the only source of DC voltage cause a LOOP.

River Bend, 458-94-023,

- Rosemont transmitters caused a spurious false high water level condition and a reactor scram. The transmitters required special dampening that the time response setting and testing maintenance instruction failed to adequately provide.

Seabrook, 443-96-003,

- Sparks were observed from the turbine driven emergency feedwater pump mechanical seal area during testing. The shaft seal design required use of non-standard maintenance practices not specified in the seal installation package.

Byron 1,454-96-007,

- Improper weld design and degraded caulk on the bus duct allowed water to enter the duct causing a trip of the Unit station auxiliary transformer, loss of off-site power, and a reactor trip. Although this information was available from another plant, work package developers failed to incorporate the lessons learned.

Callaway 483-92-011,

- During restoration of an annunciator field contact power supply that failed and was replaced, all field contact power supply fuses blew rendering all MCB annunciators inoperable. The work package failed to specify a retest for the field power supply replacement due to inadequate review of the work package and cautions contained in the procedure.

Calvert Cliffs2, 318-94-0001,

- During installation of 13.8 kV voltage regulators, an electrical protective relay inadvertently actuated causing the loss of power to two non vital and one vital safety bus and a reactor trip. At the time, a modification to install voltage regulators was thought to be functionally isolated from existing equipment. The work package control of new equipment under construction was inadequate.

Catawba 2, 414-96-001,

- Inadequate installation of bus ducting and resistor bushings caused a phase-to-phase ground fault resulting in a LOOP and reactor trip. The work package specified the wrong orientation and location for the bushings.

Fort Calhoun, 285-92-023,

- Following a high-pressure reactor trip, a pressurizer code safety valve lifted at a pressure lower than the setpoint and remained partially open. Previous failures of safety valves were not considered in work package development.
- The electrical system design precluded post maintenance testing of an invertor board replacement without placing the inverter in service. The work package failed to specify removal and reinstallation of a metal jumper that led to inverter instability, a turbine trip, and a reactor trip.

Point Beach 1, 266-94-002,

- The second of two EDGs was declared out of service because of shorting of the DC exciter voltage between the stationary and rotating electrical brush assemblies. The work package failed to specify re-lugging of all lugs as part of a recent brush jumper cable replacement.

Inadequate Maintenance Work Package and Practices

Beaver Valley 1, 334-93-013,

- While verifying auxiliary contact alignment on a switchyard main output breaker, maintenance personnel caused inadvertent actuation of an under frequency electrical breaker separation scheme, loss of electrical load, LOOP, and a reactor trip. There were no administrative operational controls over

switchgear work performed in the switchyard.

Haddam Neck, 213-93-006/007,

- Abnormal generator indications and erratic output caused an Emergency Diesel Generator to prematurely shut down during a surveillance test. Lack of scheduled maintenance or inspection for the EDG voltage regulator/excitation equipment resulted in the EDG inoperability.

LaSalle 1, 373-93-015,

- Lack of scheduled preventative maintenance on station auxiliary transformer (SAT) bus duct seals allowed water to accumulate and cause corrosion and short circuits. No drainage path for accumulated moisture existed. This condition resulted in a short circuit to ground causing loss of the station auxiliary transformer and a reactor scram.

Limerick 1, 352-95-008,

- Lack of scheduled cleaning and an insufficient Foreign Material Exclusion (FME) Program during maintenance activities in the containment allowed fouling of the RHR pump suction strainer by foreign material in the Suppression Pool.

Oconee 2, 270-97-001,

- Failure to implement an effective high-pressure injection nozzle inspection program, based on available industry recommendations, allowed a leak greater than 10 gpm to develop prompting a Technical Specification required reactor shutdown.

Perry, 440-93-011,

- An engineering evaluation determined that excessive ECCS suction strainer differential pressure may exist during long-term post-LOCA operation. Inadequate inspection processes failed to identify the problem during previous inspections and material control during maintenance activities in the containment was inadequate.

Robinson 2, 261-92-017/013/018,

- Inadequate cleanliness and foreign material control during maintenance caused blockage within a safety injection pump's minimum flow recirculation check valve and flow orifice.

Wolf Creek, 482-96-001,

- During a reactor trip caused by Frazil icing, the Turbine Driven Auxiliary Pump experienced inboard seal packing failure and was declared inoperable. The cause was loosely installed packing due to poor packing installation and adjustment.

Byron 1, 454-96-007,

- Degraded caulk on the bus duct allowed water entry causing a trip of the unit station auxiliary transformer, loss of off-site power, and a reactor trip. Although information was available, the work package failed to specify the correct procedure and maintenance failed to properly caulk the duct.

Catawba 2, 413-93-002,

- The nuclear service water system motor operated discharge valves failed to open as required during a pump start due to incorrect setting of the torque switches. The MOV set up procedure lacked information and maintenance personnel failed to consult additional available information sources.

Catawba 2, 413-96-001,

- Inadequate installation of bus ducting and resistor bushings caused a phase-to-phase ground fault resulting in a LOOP and reactor trip. The maintenance process and work package preparation installed the bushings in the wrong orientation and location.

South Texas 1, 005/007,

- Paint applied to emergency diesel generator fuel injection pumps ran into the fuel metering ports and caused binding of the fuel metering rods and a failure to start for a test. Contract painters were not adequately

supervised and did not ensure that paint did not drip into equipment.

- Failure to control foreign material introduction during maintenance caused damage to a Turbine Driven Auxiliary Feedwater Pump and system unavailability greater than the LCO allowed time.

Inadequate Maintenance Technical Knowledge

D. C. Cook 1, 315-95-011,

- A charging pump tripped on motor overcurrent after starting and operating at full flow for seven minutes due to an incorrect setting for the overcurrent relay. Inadequate continuing training in Centrifugal Charging Pump over-current calibration caused a lack of knowledge by technicians.

Limerick 1, 352-95-008,

- An insufficient Foreign Material Exclusion (FME) Program during maintenance activities in the containment and lack of scheduled cleaning allowed fouling of the RHR pump suction strainer by foreign material in the Suppression Pool. Personnel were not sufficiently knowledgeable about the effects of cleanliness on ECCS operability.

Perry, 440-93-001,

- An engineering evaluation determined that excessive ECCS suction strainer differential pressure may exist during long term post-LOCA operation. Inadequate inspection processes failed to identify the problem during previous inspections and material control during maintenance activities in the containment was inadequate. Personnel were not sufficiently knowledgeable about the effects of cleanliness on ECCS operability.

Fort Calhoon, 285-92-023,

- The work package failed to specify removal and reinstallation of a metal jumper after an inverter board replacement, which led to inverter instability, a turbine trip, and a reactor trip. Unavailability of an inverter-qualified electrician may have contributed to the event.

Inadequate Post Maintenance Testing

McGuire 2, 370-93-008,

- The turbine failed to runback as expected during a loss of electrical bus transient from a failed electrical insulator. The lack of a testing program for the turbine runback feature prevented the identification of the design and configuration problems.
- One MSIV failed to fully close after the scram causing the steam generator to boil to a dryout condition. A lack of post-modification testing on the MSIV after a modification removed additional closing force resulted in a failure to detect a significant change in the MSIV performance.

Sequoyah 1&2, 327-92-027,

- An internal fault on a newly installed switchyard power circuit breaker caused a reactor trip due to reactor coolant pump undervoltage. The testing methodology failed to appropriately assess potential risks and evaluate alternatives to testing methodology.
- Breaker testing procedures lacked adequate guidance to prevent conditions that would cause breaker failure.

Catawba 2, 413-93-002,

- The nuclear service water system MOV did not open as required during a pump start due to incorrect setting of the torque switches. Post-maintenance testing failed to properly establish correct opening of the discharge valves during the pump start sequence.

Point Beach 1, 266-94-002,

- During annual maintenance of an emergency diesel generator, a brush jumper was installed in an improper orientation causing shorting and unstable generator output. Post-maintenance testing failed to

check for proper installation and physical interference while rotating the generator.

South Texas, 498-93-005/007,

- An emergency diesel generator failed to start for a test because paint applied to the fuel injection pumps ran into the fuel metering ports and caused binding of the fuel metering rods. Contract painters were not adequately supervised and failed to ensure that paint did not drip into equipment. There was no operability testing following external activities that can effect diesel generator operability.
- Failure to control introduction foreign material during maintenance caused a Turbine Driven Auxiliary Feedwater Pump to be damaged and unavailable for greater than the LCO allowed time. The TDAFW pump was returned to service for lack of parts after finding turbine/trip throttle valve disk and stem steam cuts. On subsequent testing it tripped on overspeed. The failure to maintain consistent testing requirements may have masked turbine degradation. The equipment was not tested under actual standby conditions.

Inadequate Procedures

D. C. Cook 1, 315-95-011

- A charging pump tripped on motor overcurrent after starting and operating at full flow for seven minutes due to an incorrect setting for the overcurrent relay. Inadequate detail in the relay calibration procedure contributed to the technician error.

Hatch Unit 1, 372-00-002,

- RCIC restart procedures were inadequate.

Indian Point 2, 247-99-015, AIT 9908,

- Following a spurious reactor trip, incorrect electrical lineups and electrical equipment failure resulted in loss of vital AC, vital DC, and instrument AC power. The station auxiliary load tap changer was not maintained in the automatic position due to lack of procedural requirement to maintain compliance with the plant design basis.
- The emergency plan failed to provide adequate information, resulting in a failure to declare an unusual event.

LaSalle 1, 373-93-015,

- The electrical bus duct design failed to allow proper drainage of accumulated moisture, causing loss of the station auxiliary transformer and a reactor scram. The plant lacked procedures to back-feed buses via the unit auxiliary transformer, resulting in 29 hours to achieve back-feed.

Oconee 2, 270-92-004,

- A DC control power problem with the 230-kV switchyard caused a bus lockout and switchyard isolation. lacked emergency procedures for this and similar sequences.
- The live bus transfer, and other, procedures failed to provide adequate guidance for recovery from an improper lineup.

Sequoyah 1&2, 327-92-027,

- An internal fault on a newly installed switchyard power circuit breaker caused a reactor trip due to reactor coolant pump undervoltage. Breaker testing procedures failed to include adequate guidance for preventing conditions that cause breaker failure.

Saint Lucie 1, 335-97-011

- A loop scaling change for the refueling water tank level indication was made without a corresponding bistable setpoint change, which could have prevented performance of a safety function. Procedure change and configuration management controls during instrumentation changes were inadequate.

Wolf Creek, 482-96-001,

- Frazil icing conditions and freezing of the traveling screens caused a loss of level in the circulating water and ESWS suction bays and a reactor trip. The plant lacked procedures to identify and properly respond to Frazil icing conditions.

Catawba 2, 413-93-002,

- The nuclear service water system MOV failed to open as required during a pump start due to incorrect setting of the torque switches. Inadequate procedures failed to properly direct the correct opening of the discharge valves during the pump start sequence.

Oconee 3, 287-97-003,

- An in use HPI pump was damaged when actual LDST level dropped while both level instruments falsely indicated a constant level. No precaution existed in the shutdown/cooldown procedure warning of potential common-cause failures of LDST level instrumentation.
- Procedural guidance for failed LDST instrumentation was inadequate.
- The operations staff recognized that procedures and procedure compliance were weak but failed to take action to improve known or suspected weak procedures.

Oyster Creek, 219-92-005,

- The improper securing of a diesel generator caused a reactor scram and isolation. The operating procedure failed to incorporate information already contained in a surveillance procedure for removing a diesel generator from service without causing a reactor scram.

South Texas 1&2,498-93-005/007,

- Failure to control introduction of foreign material during maintenance damaged and rendered inoperable a Turbine Driven Auxiliary Feedwater Pump. This resulted from a lack of procedures or manuals and a failure to use best documentation for performing maintenance on safety related equipment.

Turkey Point, 250-92-001,

- The procedures for determining the parameters for seismic qualification of switchgear failed to consider the actual operational required breaker positions. The normally racked down breaker positions threatened operability of the switchgear during a seismic event.

Wolf Creek, 482-94-013,

- Operator error caused an unexpected decrease in reactor coolant level while shutdown. Procedural controls failed to prevent draining the RCS during an evolution with this potential.
- Procedures failed to caution about RCS draining from simultaneous evolutions in RHR trains.

Failure to Respond to Industry and Practices

ANO1, 313-96-005,

- One steam header safety valve failed to close after properly opening on demand after a loss of both main feed pumps (MFP) and a reactor trip. The licensee failed to act upon inspection findings and industry notices related to safety valve cotter pin and release nut problems on various safety valves in a timely manner prior to the event.

Hatch, 372-00-002,

- Tail pipe pressure switches failed to actuate as required when Safety Relief Valves (SRV) were used to reduce reactor pressure following a Scram and MSIV isolation. Industry notices for similar switches were not implemented.

Oconee 2,

- An RCS leak from a crack on the HPI to RCS cold leg nozzle sleeve forced a reactor shutdown and cooldown. Failure to incorporate industry owner group recommendations allowed ultrasonic testing to fail to detect such potential cracks.

Oconee 2, 270-92-004,

- A DC control power problem with the 230-kV switchyard caused a bus lockout and switchyard isolation. Unit 1 separated from the grid, oversped and locked out. The battery charger contained a defective Zener diode circuit. The licensee had failed to act upon problems with the Zener diode

component noted in industry and internal reviews.

Byron 1, 454-96-007,

- Water entered between an insulator and bus duct causing a trip of the Unit station auxiliary transformer, loss of off-site power, and a reactor trip. The licensee failed to incorporate information from another plant about a similar event into a work package for bus duct maintenance.

Wolf Creek, 482-94-013,

- The plant experienced an unexpected decrease in reactor coolant level while shutdown. The licensee failed to respond to industry notices and implement previous industry guidance concerning inadvertent draining of the RCS during RHR operations.

Failure to Follow Industry Practices

Haddam Neck, 213-93-006/007, AIT 9380

- An MCC was lost when an Automatic Bus Transfer relay failed to operate during surveillance testing of safety injection logic with a partial loss of power. A breaker wiring error originated from erroneous information in the breaker manual even though correct information was incorporated in another breaker manual that used identical relays.

McGuire 2, 370-93-008,

- During a reactor scram from a loss of electrical bus transient, one MSIV failed to fully close causing the steam generator to boil to a dryout condition. The licensee failed to incorporate vendor recommendations in maintenance and testing procedures after a modification removed additional closing force to the MSIVs.

South Texas 1&2,498-93-005/007,

- An emergency diesel generator failed to start for a test because paint applied to the fuel injection pumps ran into the fuel metering ports and caused binding of the fuel metering rods. The licensee failed to respond to lessons learned from industry diesel generator experience.

Failure to Trend and use Problem

Reports

Dresden 3, 249-96-004

- The reactor scrammed containment isolated due to failure of a feedwater regulating valves. One containment isolation valve unexpectedly opened due to a failed relay during reset of the containment isolation. The licensee failed to trend relay repair information across previous years, which could have prevented this failure.

Haddam Neck, 213-93-006/007, AIT 9380

- A total LOOP occurred due to a wiring error while conducting breaker trip logic testing during shutdown. Operators failed to identify the error based on abnormal indications of voltage during earlier outage activities.

Indian Point 2, 247-99-015, AIT 9908

- Work control personnel were unaware of previous spurious trips in the OT-ΔT circuit when planning work. This problem ultimately led to a reactor trip. Station personnel failed to recognize and evaluate a potential trend in RPS problems and failures.

Seabrook, 443-96-003,

- Personnel observed the turbine driven auxiliary feed pump outboard mechanical seal emitting sparks during a surveillance test. The licensee failed to effectively capture or trend lessons learned from previous problems with seal failures.

Fort Calhoun, 285-92-023,

- Following a reactor trip from high pressure, a pressurizer code safety valve lifted at a pressure lower than the setpoint and remained partially open. The licensee

failed to report and investigate multiple previous failures of safety valves.

South Texas 1&2,498-93-005/007,

- An emergency diesel generator failed to start for a test because paint applied to the fuel injection pumps ran into the fuel metering ports and caused binding of the fuel metering rods. The licensee failed to respond to lessons learned from industry diesel generator problem reports.

Failure to Correct Known Deficiencies

ANO1, 313-96-005,

- One steam header safety valve failed to close after properly opening on demand following a loss of both main feed pumps (MFPs) and a reactor trip. The licensee delayed taking action to identify and correct the root cause of the safety valve problems after a similar problem with a main steam safety valve (MSSV).
- Operator work-arounds involved manually operating the atmospheric dump isolation valve when an atmospheric dump valve failed due to binding

Dresden 3, 249-96-004

- With feedwater regulating valve A (FRV-A) was out of service because of a steam leak, FRV-B failed causing a low reactor water level, scram, and containment isolation. Poor maintenance work process prioritization, planning, and scheduling, delayed repairing and restoring FRV-A before the FRV-B failure.

Indian Point 2, 247-99-015, AIT 9908

- Work control personnel were unaware of previous spurious trips in the OT ΔT circuit when planning work. This problem ultimately led to a reactor trip. Engineering personnel failed to investigate the cause of an earlier OT ΔT signal increase.
- Corrective actions for Amptector test methodology were overdue and incomplete.

LaSalle 1, 373-93-015,

- Lack of scheduled preventative maintenance on station auxiliary transformer (SAT) bus duct seals allowed water to accumulate and cause corrosion and short circuits. This condition resulted in a short circuit, loss of the station auxiliary transformer, and a reactor scram. Design inadequacies and inappropriate maintenance were compounded by failure of the CAP to respond to a previous similar plant event.

McGuire 2, 370-93-008,

- Excessive time taken to read the EOP pages following a turbine trip and reactor trip delayed implementation of procedural steps to isolate MSIVs prior to an SI signal. Previous deficiencies during training had identified this weakness.
- The licensee failed to evaluate actions during a previous LOOP and create procedures to mitigate the main steam isolation and SI.

Oconee 2, 270-97-001,

- An RCS leak from a crack on the HPI to RCS cold leg nozzle sleeve forced a reactor shutdown and cooldown. Ultrasonic testing failed to detect potential cracks of this type.
- The CAP failed to effectively address known problems and implement appropriate corrective actions.

Salem 1, 27294007,

- Poor control of a rapid down-power evolution in response to river grass intrusion at the intake structure caused a reactor trip and SI. A modification to relieve aggravated conditions caused by river grass was planned but not implemented prior to the event.
- Operators were trained to work around unmaintained atmospheric relief valve automatic control problems.
- The automatic rod control system was not in service for a month prior to the event, requiring a manual mode of operation.

Inadequate Supervision

Indian Point 2, 247-99-015, AIT 9908,

- Following a spurious reactor trip, incorrect electrical lineups and electrical equipment failure resulted in loss of vital AC, vital DC, and instrument AC power. Station managers failed to anticipate the vulnerabilities caused by a partial loss of power and establish expectations that recovery from degraded conditions had priority over shutdown preparations.
- Station supervision failed to ensure plant staff assistance to operators in mitigating degraded plant conditions.

Limerick 1, 352-95-008,

- An insufficient Foreign Material Exclusion (FME) Program and lack of scheduled cleaning during maintenance activities in the containment allowed the RHR pump suction strainer to foul from foreign material in the Suppression Pool. Management failed to set cleanliness expectations for the containment and suppression pool.

Millstone 2, 336-95-002,

- Inadequate engineering evaluation of valve susceptibility to pressure locking and thermal binding and inadequate supervision of that evaluation allowed a common mode failure that would prevent entry into the containment sump recirculation mode.

Oconee 2, 270-97-001,

- An RCS leak from a crack on the HPI to RCS cold leg nozzle sleeve forced a reactor shutdown and cooldown. Plant operations failed to minimize thermal stresses.

Perry, 440-93-011,

- An engineering evaluation determined that excessive ECCS suction strainer differential pressure may exist during long-term post-LOCA operation. Inspection processes failed to identify the problem during previous inspections, and material control during maintenance activities in the containment was inadequate. Management failed to set cleanliness expectations for the containment and suppression pool.

Callaway, 483-92-011,

- During restoration of an annunciator field contact power supply that failed and was replaced, all field contact power supply fuses blew rendering all MCB annunciators inoperable. Repair work was signed as complete though 164 annunciators remained inoperable. The I&C technicians were unsupervised during the power supply replacement and blown fuse trouble-shooting.

Salem 1, 272-94-007,

- Control room operators lacked management guidance during a plant power reduction in response to river grass intrusion at the intake structure.
- A rapid down power evolution with multiple reactivity changes was poorly controlled. The NSS gave the reactor operator vague directions to pull rods to restore Tave. The RO's Requests for additional information were not treated seriously.
- A reactor operator was incorrectly directed to leave the reactor console controls when reactivity was unstable.

South Texas 1&2,498-93-005/007,

- An emergency diesel generator failed to start for a test because paint applied to the fuel injection pumps ran into the fuel metering ports and caused binding of the fuel metering rods. Contract painters lacked adequate supervision, allowing their activities to affect diesel generator operability.

Inadequate Knowledge of System

Indian Point 2, 247-99-015, AIT 9908,

- Following a spurious reactor trip, incorrect electrical lineups and electrical equipment failure resulted in loss of vital AC, vital DC, and instrument AC power. Station managers failed to anticipate the vulnerabilities caused by the loss of power.

- Lack of Technical Specification knowledge caused late entry into a TS LCO.
- Knowledge of the regulatory requirements and safety design basis for maintaining the transformer load tap changer in automatic was lacking.

Organizational Structure

Saint Lucie 1, 335-97-011
A loop scaling change for the refueling water tank level indication was made without a corresponding change to the bistable setpoint, which could have prevented performance of a safety function. The organizational structure placed responsibility for fully implementing changes across multiple organizations due to inadequate procedural change and configuration management control during instrumentation changes.

APPENDIX C

DEFINITION OF HUMAN PERFORMANCE INFLUENCE FAILURE SUBCATEGORIES USED IN THE REVIEW OF OPERATING EVENTS

C1. Operations

1. Command & Control Including Resource Management - 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 (Ops) - 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.

C2. 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 and 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.

C3. Maintenance Practices and Maintenance

10. Work Package Development, QA & Use - The work package preparation was deficient in some way, including quality assurance 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 - Testing performed after maintenance was inadequate or insufficient to correctly determine the operability of the equipment after the maintenance was considered complete.

C4. Inadequate Procedures/Procedure Revision

14. Inadequate Procedures or Procedure Revision - 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.

C5. CAP and Learning

15. Fail 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.

C6. 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.

APPENDIX D

INSPECTION PROCEDURE MAPPING TO HUMAN PERFORMANCE FINDINGS

D1. Comanche Peak (LER 445-95-003/4) - Loss of Feedwater Leading to Reactor Trip

From Group 1: Design and Maintenance

Event Synopsis/Elements

On June 11, 1995 the Comanche Peak Unit 1 balance of plant reactor operator (utility licensed) was performing the train A slave relay test for the K601A relay. During the test, a non safety related inverter unintentionally 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. The inverter static switch is designed to prevent transfer to a de-energized power source but malfunctioned by effecting the transfer. This resulted in loss of power to auxiliary relays, which caused a false main feedwater pump low oil pressure signal that tripped both condensate pumps. The loss of the condensate pumps resulted in an automatic trip of both main feedwater pumps. Control board indication and alarms alerted the reactor operator that there was a loss of feedwater. A manual reactor trip of Comanche Peak Unit 1 was initiated due to the loss of feedwater to the steam generators.

On unit 1, one MDAFW pump started as required but the other MDAFW pump was aligned to the test header for the slave relay testing. The TDAFW pump started and immediately tripped on overspeed. This caused less than the design required feed to the steam generators.

Subsequently, the 72-hour outage time for making the unit 1 turbine driven auxiliary feedwater pump "operable" was exceeded.

Within a week, the unit 2 TDAFW pump was also declared inoperable during surveillance testing when it too tripped on overspeed. No adverse plant effects occurred.

Elements: The cause of both the inverter failures and TDAFW pump failures were the result of failures in design and maintenance practices.

Human Failures Contributing to the Event

Design

There was a failure in the design of the main feed pump (MFP) power trip relays to prevent power loss to the relays from causing the condensate pumps to trip on a false MFP low lube oil pressure signal.

The transient power transfer protection for the inverter was inadequately designed to prevent transfer to a de-energized source.

The governor valve stem on both unit 1 and unit 2 TDAFW pumps experienced corrosion, in part due to poor choice of stem materials, which contributed to the inability to control speed. Both were replaced with a stem made of Inconel that was a better choice for this application in an adverse environment.

Cornerstone attribute: design (original)
Applicable IP's: 71111.21, system design capabilities
Applicable PI: none

Maintenance

Non-safety related inverter components were not calibrated. The licensee failed to calibrate the static switch logic sense printed circuit board and analog boards for non-safety related inverters to prevent transients from defeating the reverse lockout circuitry causing the inverter to transfer to a deenergized power source.

The unit 1 TDAFW pump tripped on overspeed due to governor valve stem corrosion causing binding of the stem in conjunction with slight binding of the governor valve cam linkage assembly. Maintenance failed to detect stem corrosion.

The unit 2 TDAFW pump tripped on overspeed due to water in the steam lines, remaining from an earlier warm up run. The water when combined with slight binding of the governor cam linkage from existing stem corrosion restricted movement and left the governor incapable of controlling speeds. Maintenance had failed to detect and correct water remaining from degraded steam traps.

Cornerstone attributes: Equipment performance, reliability; Procedure quality, maintenance and testing (pre-event)
Applicable IP's: 71111.12 maintenance rule implementation, 71111.19 post maintenance testing, and 71111.22 surveillance testing
Applicable PI: safety system functional failures

D2. Catawba (LER 413-93-002) -Emergency Service Water Potentially Unavailable

From Group 2: Design, Maintenance, and Operations

Event Synopsis

On February 25th, 1993, at Catawba Units 1 and 2 the Nuclear Service Water (NSW) discharge valves for "B" train failed to open during NSW water pump start. These valves are designed to automatically open following pump start. Technical Specification 3.03 was entered for Unit 1 operating at power with potentially both trains of nuclear service water being unavailable. A loss of NSW affects the facility capability to respond to LOCA events. Unit 1 NSW pump discharge valves were previously set up in 1992 and tested with requirements of Generic Letter 89-10. Unit 2 pump discharge valves set up and testing was scheduled in May 1994.

During the period of time between August 1992 through February 1993, three of the four NSW pump discharge valves, which supply all NSW to both units, were unable to open against full differential pressure. Although the torque switch setting (TSS) for unit 1 were properly set at maximum, the TSS for unit 2 remained improperly set at a lesser value. These multiple failures result in a potential loss of all NSW to both units.

The cause of the unit 1 valves (MOV) failing to open was attributed to sizing variables that are possibly inadequate for this specific application and/or possible degraded valve subcomponents. The cause of the unit 2 valves (MOV) failing to open was incorrect torque switch settings resulting from a lack of detailed information in the MOV torque switch set up procedure. Additionally, the "open" and "close" switches were not clearly identified or marked within the MOV. In effect, the torque limits were reached and thus the torque switches were opened, thus stopping additional valve movement prior to the valve being able to open.

Furthermore, when nuclear service water is declared inoperable, technical specifications require both diesel generators (DGs) to be declared inoperable and to perform a specific surveillance called out by TS. This surveillance was not performed within the required time. Policy guidance was not well defined or understood relative to the need to perform the surveillance test when in TS 3.0.3. Operations incorrectly assumed that TS 3.0.3 was more restrictive and that the surveillance test specified elsewhere in TS was not necessary.

Elements: Cause of valve failure was incorrect torque settings and inadequate design considerations.

Human Failure Contributions to the Event

Design

Incorrect setting of the torque switches were in part, the result of non-existent "open" and "close" markings on the MOV internals.

The licensee had incorrect manufacture sizing calculations for flow and pressure conditions in order to properly establish TSS and ensure that the MOVs will open under full expected flow conditions.

Cornerstone attribute: design (original); Procedure quality (pre-event)
Applicable IP's: 71111.21, system design capabilities
Applicable PI: none

Maintenance

Although maintenance procedures were not explicit and there were no torque switch labeling within the MOV, maintenance knowledge and practices for setting MOV torque switches were deficient and allowed incorrect TSS without question.

Cornerstone attributes: Procedure quality, maintenance and testing (pre-event)
Applicable IP's: 71111.19 post maintenance testing, 71111.22 surveillance testing
Applicable PI: safety system functional failures

Procedure

A lack of detailed information existed on the approved MOV torque switch set up process contained in the maintenance procedure.

The policy guidance was not well defined or understood relative to the requirement to perform the surveillance test specified by another section of TS, when already in TS 3.0.3.

Cornerstone attributes: Procedure quality, maintenance and testing (pre-event)
Applicable IP's: 71111.19 post maintenance testing, 71111.22 surveillance testing
Applicable PI: safety system functional failures

D3. Haddam Neck (LER 213-93-006/007/009/010 and AIT 93-080) - Logic Tests Leading to a Total LOOP and Partial Loss of Vital Power

From Group 3: Design, Maintenance, Operations, and CAP

Synopsis of five related events

On June 22, 1993, Haddam Neck was in cold shutdown. During breaker failure trip logic testing on the offsite power tiebreaker, the station experienced a total LOOP. In response to the LOOP, both emergency diesel generators (EDGs) automatically started and provided emergency power to the station. At the time of the event, shutdown cooling was temporarily lost. The root cause for this event was identified as a wiring error in offsite power tiebreaker failure trip logic that wrongly tripped the remaining offsite supply breaker. 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, which included actually tripping the input supply breakers.

On June 26, 1993, Haddam Neck was in the refueling mode. While performing surveillance testing of Train A of the safety injection logic with an intentional partial LOOP, a complete LOOP occurred. In response to the LOOP, both emergency diesel generators (EDGs) automatically started and shutdown cooling was restored. The root cause of this failure was determined to be a blown fuse that was not annunciated or identified before the test. The fuse was known to be good within a week prior to the test. Fuses are not typically checked as a test prerequisite. When Train A power was intentionally de-energized, the remaining supply breaker tripped open as designed, due to the lack of sensed voltage because of the blown fuse.

Three related occurrences were involved in this event:

On June 27, 1993, during surveillance testing of a protected train of the safety injection actuation logic with a partial LOOP, a temporary loss of MCC-5 occurred when the automatic bus transfer scheme failed to operate. The most likely cause was determined to be intermittent failure of either of two relay components within associated power supply breakers.

On May 25, 1993, Emergency Diesel Generator A was manually shut down after 22 hours of a 24 hour test run. Erratic diesel output and abnormal generator indications prompted the premature shutdown. Investigation showed that the generator field excitation cabinet had inadequate cooling which led to failure of the rectifier assembly and loss of the generator field. The high electrical loading coupled with excess dust accumulation, loss of forced ventilation to the cabinet, and component age all contributed to the failure.

On May 25, 1993, it was discovered that the air receiver pressure for the power-operated relief valves (PORVs) decayed faster than allowed by Technical Specifications. The root cause was due to a malfunction of the air dryer supplying the receiver and was compounded by a lack of indication of dryer performance and error in the valve lineup for instrumentation that may have allowed detection of the malfunction prior to failure.

Human failures contributing to the Events

LOOPS

Item #1 - The wiring of an offsite electrical power breaker was incorrect, which apparently occurred during or shortly following plant construction. Configuration management and drawing control as well as past failure to adequately test power supply breaker logic, all contributed to the LOOP.

Cornerstone Attributes: design (original)
Applicable IPs: 71111.21, Safety System Design and Performance Capability Procedure
Applicable PIs: None

Inspection of safety system design and performance verifies the initial design and subsequent modifications and provides monitoring of the capability of the selected system to perform its design basis functions.

Item #2 - A blown fuse that was not annunciated or checked prior to surveillance testing of the safety injection logic caused a complete LOOP. The following human errors contributed to this event:

1) Attributing failures to the wrong component. Because of inadequate technical knowledge, operators failed to fully investigate and properly identify previous breaker failures based on abnormal indications during earlier outages.

2) Personnel incorrectly believed that there was a problem with a voltage switch instead of believing that the failed component was a blown fuse.

3) Operator technical knowledge was deficient in that they failed to reset the safety injection relays in order to restore safety injection after the LOOP.
Cornerstone attributes: Human performance (human error, pre-event, post event)
Applicable IPs: 71152 PI&R, 71153 Event Follow-up
Applicable PIs: scrams, transients, and safety system unavailability

71153 01.01 Evaluate licensee events and degraded conditions for plant status and mitigating actions in order to provide input to determining the need for an Incident Investigation Team (IIT), Augmented Inspection Team (AIT), or Special Inspection.

01.02 Screen event reports that licensees are required to submit to the NRC for significance and obvious violations.

MCC (Distributed Motor Control Center)

Item #3 - Deficient maintenance practices allowed the snap rings for the distributed motor control center to be improperly installed.

Cornerstone attributes: equipment performance (reliability, availability)
Applicable IP's: 71111.12 Maintenance Rule implementation, 71152 PI&R

Applicable PIs: safety system functional failures, safety system unavailability

Item #4 - The licensee failed to perform an adequate root cause analysis to correctly identify the breaker that had failed.

Cornerstone attributes: human performance (pre-event)
Applicable IPs: 71111.13 Maintenance Rule Risk Assessment and Emergent Work, 71152 PI&R
Applicable PIs: none

71111.13	02.03 Problem Identification and Resolution. Verify that the licensee is identifying problems with maintenance-related risk assessment and management and emergent work control and entering them in the CAP. For a sample of significant problems documented in the CAP, verify that the licensee has identified and implemented appropriate corrective actions. See Inspection Procedure

Item #5 - In the presence of time constraints, operators failed to verify information including control room indication. As a result they issued an incorrect emergency classification to the state.

Cornerstone attributes: ERO performance
Applicable IPs: 71114 Emergency Preparedness and 71111.11 licensed operator requalification
Applicable PIs: none

Item #6 - Lack of vendor configuration management in combination with licensee lack of review between like manuals resulted in dissimilar vendor manuals for relay information.

This area not addressed under the new program

Item #7 - Engineering evaluation did not fully investigate previous failures with the same MCC relay to determine a positive root cause of similar events.

Cornerstone attributes: PI&R
Applicable IPs: 71111.13 Maintenance Rule Risk Assessment and Emergent Work, 71152 PI&R
Applicable PIs: none

71111.13	02.03 Problem Identification and Resolution. Verify that the licensee is identifying problems with maintenance-related risk assessment and management and emergent work control and entering them in the CAP. For a sample of significant problems documented in the CAP, verify that the licensee has identified and implemented appropriate corrective actions. See Inspection Procedure 71152, "Identification and Resolution of Problems," for additional guidance.

EDG Failure

Item #8 - Maintenance failed to maintain adequate cleanliness of the generator voltage regulator field cabinet. Reduced heat removal from the cabinet leading to component failure resulted.

Cornerstone attributes: configuration control (equipment line up)
Applicable IP's: 71111.04 Equipment Alignment, 71111.12 maintenance rule implementation
Applicable PIs: none

71111.14 02.02 Complete Walkdown

a. Select a risk-important mitigating system. Consider site-specific risk study, plant mode, and previous walkdowns.
b. Review documents to determine correct system lineup. Consider plant procedures including abnormal and emergency operating procedures, drawings, the updated final safety analysis report, and vendor manuals.
c. Review outstanding maintenance work requests on the system and any deficiencies that affect the ability of the system to perform its function.
d. Review outstanding design issues including temporary modifications, operator workarounds, and items tracked by engineering department.
e. Perform walkdown. Identify any discrepancies between existing system equipment lineup and correct lineup. Listed below are examples of items to review during the walkdown.

1) Valves are positioned correctly and do not exhibit leakage that would impact the valve's function
2) Electrical power is available as required
3) Major system components are correctly labeled, lubricated, cooled, ventilated, etc.
4) Hangers and supports are correctly installed and functional
5) Essential support systems are operational
6) Ancillary equipment or debris does not interfere with system performance

Item #9 - Engineering design did not consider the long-term capability of cooling equipment. The field exciter cabinet cooling air fans were run continuously instead of only when needed. This is not specifically addressed by the new inspection program, but could be covered under 71111.21, safety system design and functional capability.

Item #10 - Engineering evaluation was performed without due consideration of plant aging effects for electrical component failures in a poorly cooled environment. This contributed to field circuit failure.

Same as response to Item #8 - Once the cooling deficiency was identified, engineering should have addressed the lack of cooling on electronic aging.

PORV Failure

Item #11 - Engineering design did not provide for a means to indicate air dryer malfunction by reduction of air dryer performance. Water entered the system and deteriorated the diaphragm, and was not detected until adverse effect on PORV operation occurred.

Cornerstone attributes: design (original)
Applicable IP's: 71111.21 safety system design and capability, 71153 Event Follow-up
Applicable PIs: none

71153 01.01 Evaluate licensee events and degraded conditions for plant status and mitigating actions in order to provide input to determining the need for an Incident Investigation Team (IIT), Augmented Inspection Team (AIT), or Special Inspection.

01.02 Screen event reports that licensees are required to submit to the NRC for significance and obvious violations.

Item #12 - An error in the valve lineup by operators for air dryer instrumentation may have prevented detection of the dryer malfunction and correction of the deficiency prior to failure.

Cornerstone attributes: configuration control (equipment alignment–at power)
Applicable IP's: 71111.04 Equipment Alignment
Applicable PIs: safety system unavailability

Inspection Bases: Systems or components that are not properly aligned can lead to the initiation of an event and can impact the availability and functional capability of plant equipment, which could significantly increase the overall risk to the plant. Inspection activities would normally be performed following emergent work activities and planned removal of risk significant systems for on-line maintenance.

71111.04-01 Inspection Objectives

01.01 To verify equipment alignment and identify any discrepancies, which impact the function of the system and therefore potentially increase risk.

01.02 To verify that the licensee has properly identified and resolved equipment alignment problems that cause initiating events or impact mitigating system availability.

D4. Fort Calhoun (LER 285-92-023) - - Reactor High Pressure Trip and LOCA

From Group 3: Design, Maintenance, Operations, and CAP

Event Synopsis

On July 3rd, 1992 Fort Calhoun received two Inverter #2 Trouble Alarms, which cause the inverter to automatically shift to the "Bypass" mode. These subsequently cleared without corrective action. Upon receipt of the third "Bypass" alarm (all within 12 hours), the inverter was manually bypassed for repair and replacement of electronic control boards. When returned to service following repairs, Inverter #2 began cycling between its two power supplies. This resulted in inverter output voltage oscillations and caused various undesirable effects but most importantly caused the electrical supply breaker to the panel for the turbine EHC Supervisory Panel to trip open. When power was lost, four pressure transmitters became de-energized and which caused the main turbine control valves to close but this action does not result in a automatic turbine trip.

Because the turbine did not trip to enable full use of the steam dump and bypass system, and with the control valves closed, the heat sink for the RCS was lost. The turbine bypass system was limited in capacity to approximately 5%. The large mismatch between reactor power and steam demand caused a sharp increase in RCS temperature, pressurizer level, pressurizer pressure and steam generator pressure. Pressurizer PORVs, Main Steam Safety Valves, and possibly one pressurizer code safety valve opened at this time to reduce RCS pressure. Due to the high reactor pressure, the reactor and turbine tripped. RCS pressure then decreased allowing the PORVs and main steam safety valves (MSSVs) to close. The pressurizer code safety valve was not recognized by operators as having lifted or leaking at this time. It was discovered only during post event analysis.

Plant parameters stabilized and RCS pressure was recovering from a low of 1745 psia. When RCS pressure increased to approximately 1923 psia, one pressurizer safety valve lifted and subsequently closed at approximately 1020 psia, but due to damage, it did not reseat. This caused an approximate 200 gpm leak (SBLOCA) to the quench tank throughout the remainder of the event and eventually ruptured the pressurized quench tank rupture disk. The operator shut the PORV block valves when quench tank level was observed to rise to but no avail and the safety valve tailpipe temperature alarm indicated leakage from the pressurizer safety valve. Pressure drop continued and SI

and containment isolation signals were received. The open pressurizer code safety valve partially closed at 1,000 psia and a plant cooldown was initiated in accordance with established procedures.

Elements:

The cause of the reactor trip was inverter failure caused by improper maintenance.
The cause of the LOCA from pressurizer code safety valve failure was improper maintenance and design.

Design and Maintenance Human failures contributing to the event

Design

Item #1- The Electro hydraulic Control power supply to the pressure transmitters was changed to a safety related source when pressure transmitters were replaced with a new design but they did not have a backup supply from the PMG as the original design had.

Cornerstone attributes: design (original, modifications)
Applicable IP's: 71111.21, Safety System Design and Performance Capability Procedure; 71111.17, permanent plant mods
Applicable PIs: none

Inspection of safety system design and performance verifies the initial design and subsequent modifications and provides monitoring of the capability of the selected system to perform its design basis functions.

Item #2 Sufficient turbine trips for loss of load did not exist which would have enabled the steam dump and bypass system to help mitigate the power mismatch when the turbine control valves closed (apparently an original design weakness).

Cornerstone attributes: design (original)
Applicable IP's: 71111.21, Safety System Design and Performance Capability Procedure;
Applicable PIs: none

Inspection of safety system design and performance verifies the initial design and subsequent modifications and provides monitoring of the capability of the selected system to perform its design basis functions.

Item #3 The pressurizer code safety valve design and piping configuration could not tolerate vibrations caused by liquid in the instrument loop seal. This caused damage to the valve internals and bellows assembly, which did not allow the safety valve to reseat properly.

No IPs cover this issue; Other generic communication such as Information Notices may address this.

Item #4 The vibration from the lifting safety relief valve loosened the set point adjusting bolt locknut allowing the pressure set point adjusting bolt to back out and reduce the lifting pressure set point when the relief actuated. In addition there was no mechanical locking device on the pressure adjustment bolt locknut to prevent mechanical release of the adjusting bolt.

No IPs cover this issue; Other generic communication such as Information Notices may address this.

Item #5 Because consideration of maintenance test requirements in the design phase was inadequate, there was no way to perform maintenance and post-maintenance testing on an isolated inverter without losing power to the bus and subsequently placing the inverter in service.

Cornerstone attributes: design (original)
Applicable IP's: 71111.21, Safety System Design and Performance Capability Procedure
Applicable PIs: none

Inspection of safety system design and performance verifies the initial design and subsequent modifications and provides monitoring of the capability of the selected system to perform its design basis functions.

CAP

Item #6 A number of previous safety valve failures were unreported and not investigated. A review of records revealed that the as-found set points of pressurizer code safety valves have been outside their required set pressures on many previous occasions.

Cornerstone attributes: Design (original), equipment performance
Applicable IP's: 71111.21, Safety System Design and Performance Capability Procedure, 71111.12, maintenance rule implementation, 71111.22 surveillance testing
Applicable PIs: safety system functional failures, safety system unreliability

71111.21 Section 02.03 (Identification and Resolution of Problems) Verify that the licensee is identifying design issues at an appropriate threshold and entering them in the CAP. As it relates to design issues, select a sample of problems in the selected system(s) and other risk-significant systems documented by the licensee, and verify effectiveness of corrective actions. See Inspection Procedure 71152, "Identification and Resolution of Problems," for additional guidance.

71111.22 Inspection of this area ensures that safety systems are capable of performing their safety function and would support the Mitigating Systems and Barrier Integrity Cornerstones. The failure to identify and resolve performance degradation of structures, systems and components, could result in long periods of unknown equipment unavailability. This inspectable area verifies aspects of the associated cornerstones not measured by performance indicators.

Maintenance

Item #7 Inadequate prior maintenance on Inverter #2 resulted in a reactor trip during inverter restoration to service.

The LER cites as contributing causes lack of a troubleshooting guide, poor workmanship during manufacture, and unavailability of an inverter qualified electrician during repairs.

Cornerstone attributes: human performance, equipment performance
Applicable IPs: 71111.22, Maintenance Risk Assessments and Emergent Work Evaluation
Applicable PIs: scrams

Paragraph (a)(4) of 10 CFR 50.65, the Maintenance Rule (MR), requires licensees to assess and manage plant risk related to maintenance activities during all modes of plant operation. Risk is assessed and managed for both scheduled maintenance and emergent work. Risk management minimizes risk-significant configurations and initiating events and maximizes availability of mitigating systems and barriers to radiological releases.

Item #8 Inadequate prior maintenance in securing the set point bolt locknut and poor piping design for pressurizer code safety valves resulted in the safety valve prematurely lifting and failing to reseat. This caused a small break LOCA from the pressurizer.

Cornerstone attribute: equipment performance
Applicable IPs: 71111.12, maintenance rule implementation
Applicable PIs: none

Item #9 Vendor information was not requested regarding correct circuit board configuration. When the static switch drive board was replaced, a metal jumper was not identified to be installed on the new board. This missing metal jumper caused the inverter to oscillate between forward and reverse.

Cornerstone attributes: design (original)
Applicable IP's: 71111.21, Safety System Design and Performance Capability Procedure
Applicable PIs: none

Inspection of safety system design and performance verifies the initial design and subsequent modifications and provides monitoring of the capability of the selected system to perform its design basis functions.

Item #10 Prior improper maintenance resulted in a wire feeding the signal from the static switch drive board to the gate of the inverter to be loose. This caused one SCR to not gate on, resulting in a zero voltage signal which contributed to the voltage fluctuations between 120V and zero. In addition, failure in the work package preparation allowed for the metal jumper between points 6 and 7 of TB 204b to be missed and not reinstalled during replacement of the inverter board.

Cornerstone attributes: design, procedure quality (maintenance and testing)

Applicable IP's: 71111.21, Safety System Design and Performance Capability Procedure; 71111.19 post maintenance testing
Applicable PIs: safety system functional failures
Inspection of safety system design and performance verifies the initial design and subsequent modifications and provides monitoring of the capability of the selected system to perform its design basis functions.
Inspection of post maintenance testing verifies that the testing procedures assure proper functioning of equipment maintained.

Procedures

The pressurizer code safety valve refurbishment procedure was inadequate to document proper tightening of the set point adjusting bolt locknut.

Operations

Item #11 The functional recovery was complicated by human interface problems including absent or conflicting information. Three annunciator panels were de-energized and one pressure indicator was indicating zero when the other two were at 100%. This made operator response more difficult.

The control room indication did not adequately inform the crew that a safety valve had failed to reseat until closure of the PORV blocking valves did not stop the quench tank level increase.

As a result of control room indications lost due to the inverter output oscillations, operator diagnosis was hampered by malfunctions in computer displays for containment temperature and RCS subcooling parameters.

There were excessive distances between related controls and displays that hindered control room operator evaluation and mitigation of events in progress.

Cornerstone attributes: human performance (post events)
Applicable IP's: 71111.14 personnel performance during non-routine events, 71153 Event Follow-up
Applicable PIs: none

71153	01.01 Evaluate licensee events and degraded conditions for plant status and mitigating actions in order to provide input to determining the need for an Incident Investigation Team (IIT), Augmented Inspection Team (AIT), or Special Inspection.
	01.02 Screen event reports that licensees are compulsory to submit to the NRC for significance and obvious violations.

APPENDIX E

FACILITY INSPECTION REPORTS

This appendix presents findings regarding human performance issues present in inspection reports for a sample of pilot and non-pilot plants. Tables E-1 and E-2 compare findings and issues present in pilot and non-pilot inspection reports, respectively. Section E.1 presents summary human performance findings related to the reports for non-pilot plants.

Table E-1. Performance failure category frequency for pilot inspection reports .

	Command & Control Including Resource	Failure to Follow Safe Work Practices	Inadequate Knowledge or Training (Ops)	Incorrect Operator Action/Inaction	Cont. to Operate During Unstable Conditions	Communications	Design Deficiencies	Design Change Testing	Inadequate Engineering Evaluation/Review	Ineffective Abnormal Condition Indication	Configuration Management	Work Package Development, QA & Use	Inadequate Maintenance Work Packages &	Inadequate Technical Knowledge (Maint.)	Inadequate Post-Maintenance Testing	Inadequate Procedures/Procedure revision	Fail to Respond to Industry & Internal	Failure to Follow Industry Practices	Failure to Identify by Trending & Use	Failure to correct known deficiencies	Inadequate Supervision	Inadequate Knowledge of Systems	Organizational Structure
	Operations						Design and Design Change Work Practices					Maintenance Practices and Maintenance Work Control					Corrective Action Program and Learning				Manage-ment Oversight		
Summary Inspection Findings for 4 Pilot Plant Facilities (Fitzpatrick, Prairie Island, Sequoyah 1 &2, and Cooper)	3		2	5			5		4		9	3	5	1	4	14	7				2		

Table E-2. Failure category findings for non-pilot plant inspection reports.

Non-Pilot Facility & Inspection Report #	Operations						Design and Design Change Work Practices					Maintenance Practices and Maintenance Work Control					Corrective Action Program and Learning				Manage-ment Oversight		
	Command & Control Including Resource Management		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 Work Packages & Practice	Inadequate Technical Knowledge (Maint)	Inadequate Post-Maintenance Testing	Inadequate Procedures/Procedure revision	Fail to Respond to Industry & Internal	Failure to Follow Industry Practices	Failure to Identify by Trending & Use	Failure to correct known deficiencies	Inadequate Supervision	Inadequate Knowledge of Systems	Organizational Structure
Beaver Valley 1&2 00-05									L				L		L								
Browns Ferry 00-03			A	A									L			L							
Brunswick 1&2 00-03																L							
Calloway 00-10			A						L														
Calvert Cliffs 00-04							L						L			L							
Clinton 00-12													L										
Davis Besse 00-03				A																			
Diablo Canyon 00-09			A	A			L						A										
Dresden 2&3 00-07				A																L			
Duane Arnold 00-02							L									L							
Farley 00-03				A							L									L			
Nine Mile Pt 1&2 00-04	L																						

	Command & Control Including Resource Management		Inadequate Knowledge or Training (Ops)	Incorrect Operator Action/Inaction		Communications	Design Deficiencies	Design Change Testing	Inadequate Engineering Evaluation/Review	Ineffecuve Abnormal Condition Indication	Configuration Management	Work Package Development, QA & Use	Inadequate Maintenance Work Packages & Practice	Inadequate Technical Knowledge (Maint.)	Inadequate Post-Maintenance Testing	Inadequate Procedures/Procedure revision	Fail to Respond to Industry & Internal	Failure to Follow Industry Practices	Failure to Identify by Trending & Use	Failure to correct known deficiencies	Inadequate Supervision	Inadequate Knowledge of Systems	Organizational Structure
North Anna 00-08																	L		L				
Oconee 1,2&3 00-05			A	A					L				A		L	L				L			
Oyster Creek 00-05				A		A							A			L							
Palisades 00-07				A																			
Point Beach 00-06									L														
River Bend 00-10									L			L			L								
San Onofre 00-06			A						L				L	L						L		L	
South Texas 1&2 00-09															L								
Susquehanna 00-03				A								L	L										
TMI 00-04				A											L					L			
V. C. Summer 00-03									L						L								
WNP-2 00-10				A					L			L	L		L				L				

Appendix F

Table F-1. Summary ROP inspection findings for Indian Point 2.

Failure	Cornerstone	Date
Higher failure rate on requalification examinations.	Initiating events	11/18/00
Inadequate records of licensed operator attendance at requalification training.	Initiating events	11/18/00
Failure to sample all senior reactor operators (SROs) on emergency plan implementation.	Initiating events	11/18/00
Failure to identify and correct a significant condition adverse to quality involving the presence of primary water stress corrosion cracking in steam generator tubes.	Initiating events	7/20/00
Failure to maintain RCS cooldown rate within required Tech Spec Limits following tube leak in steam generator.	Initiating events	5/26/00
Failure to validate and verify an EOP change.	Initiating events	5/26/00
General procedure inadequacies.	Initiating events	5/26/00
Supply breaker failure results in aux feed pump failure to start. CAP program and maintenance program had opportunities to consider high contact resistance in the breaker closing circuit prior to the demand failure's occurrence.	Mitigating systems	11/18/00
Following replacement of the battery bank, the batteries failed a modified performance test when capacitance was dropped. There were cell plate material problems and the battery had failed capacity tests on three separate occasions.	Mitigating systems	11/18/00
Utility tunnel functionality assessment determined that mechanical and electrical components were degraded due to inadequate support and corrosion from ground water ingress into the tunnel.	Mitigating systems	11/18/00
Inadequate fire fighting strategy for aligning fire suppression water to containment.	Mitigating systems	9/30/00
Damaged service water pump and motor control center 21 power cables.	Mitigating systems	7/1/00
Failure to correct deficiencies associated with steam generator nitrogen 16 monitors. Failure to take timely corrective actions.	Mitigating systems	5/26/00
Safety evaluation for modification of the chemical volume and control system was incomplete.	Mitigating systems	5/26/00
Degradation of boraflex panels placed the plant condition outside the design basis.	Mitigating systems	5/20/00
Failure to maintain design control of the manipulator crane control circuits. Circuit wiring was not in accordance with the controlled drawings and a jumper was being used to bypass a safety feature in the control circuit.	Mitigating systems	5/20/00
During reroute of the nitrogen piping to the reactor coolant drain tank, workers failed to perform walkdown, pre-job brief, and review of drawings. By mistake workers cut the nitrogen supply line to safety injection accumulators and PORVs.	Miscellaneous	9/30/00
Failure to perform timely resolution of degraded conditions for risk significant gas turbines. Included were failure to approve final calculation for charging pump seal water tank, coupled with poor operability determination.	Mitigating systems	5/26/00

Table F-2. Summary ROP finding for Harris.

Failure	Cornerstone	Date
Inadvertent safety injection during shutdown from conflicting activities that were the result of a breakdown in work process scheduling and implementation.	Initiating events	9/30/00
Inaccurate risk assessment for startup transformer.	Mitigating systems	12/30/00
Failure to take corrective actions after multiple trips of the emergency services chilled water chiller. Licensee's corrective actions were in error and rendered the chiller inoperable.	Mitigating systems	12/30/00
Violation of Tech Specs resulting from having only one charging/safety injection pump (CSIP) operable for a time in excess of the LCO.	Mitigating systems	9/30/00
Tech spec violation due to inoperable ECCS flow path. 2 non-cited violations, failure of valve 1RH-25 to open during surveillance test. After noticing that failure to perform post modification testing had contributed to the inoperability, the licensee failed to test other valves that had undergone modification.	Mitigating systems	9/30/00
Failure to maintain adequate procedures for fire barriers.	Mitigating systems	4/1/00
Failure to set goals and monitor the steam dump systems under the maintenance rule (10 CFR 50.65) following functional failures of the low-low reactor coolant temperature interlock to dump valves had occurred.	Mitigating systems	4/1/00
Spent fuel pool water level not maintained greater than 23 feet above stored assemblies as required by Tech Spec. 3.9.11.	Miscellaneous/ Barrier	2/19/00

Table F-3. Summary ROP findings for Oconee 1.

Failure	Cornerstone	Date
Inadequate corrective actions on BWT level instrumentation following freezing of a borated water storage tank level sensing line in 1996.	Mitigating systems	12/30/00
Reactor Protection System (RPS) trip setpoints outside allowable limits. Three channels of the RPS must be operable for the turbine trip and loss of main feedwater functions.	Mitigating systems	12/30/00
Failure to update the UFSAR and Tech Spec Bases to include standby shutdown facility equipment interdependencies that effect operability.	Mitigating systems	12/30/00
Failure to adequately perform valve alignment procedures when isolating SSW header.	Mitigating systems	9/30/00
Failure to follow work control procedures for delaying planned maintenance on Unit 3 Standby Breaker S1-3 and performing preventive maintenance out of sequence.	Mitigating systems	7/1/00
Seven apparent violations related to the emergency feed water systems design. Past design not functional for a main feed water line break. Modification on emergency feedwater (EFW) valves was such that all 3 EFW pumps would automatically take suction from a drained down upper surge tank (UST) resulting in the loss of EFW system flow when the pump suction water was lost.	Mitigating systems	7/1/00
Failure to be able to open low-pressure injection valves LP-17 and LP-18 within required time constraints following a LOCA.	Mitigating systems	4/7/00

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

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

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

NUREG/CR-6775

2 TITLE AND SUBTITLE

Human Performance Characterization in the Reactor Oversight Process

3 DATE REPORT PUBLISHED

MONTH	YEAR
September	2002

4 FIN OR GRANT NUMBER

E-8238

5 AUTHOR(S)

D. I. Gertman, B. P. Hallbert, D. A. Prawdzik

6 TYPE OF REPORT

Technical

7 PERIOD COVERED *(Inclusive Dates)*

5 Aug 1999 - 25 Sep 2001

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

Idaho National Engineering and Environmental Laboratory
P.O. Box 1625
Idaho Falls, ID 83415-3129

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

Division of Systems Analysis and Regulatory Effectiveness
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10 SUPPLEMENTARY NOTES

E. A. Trager, NRC Project Manager

11. ABSTRACT *(200 words or less)*

This report documents results of a review of the Reactor Oversight Process (ROP) and its characterization of human performance that was performed by the Idaho National Engineering and Environmental Laboratory (INEEL) to describe the means by which the Nuclear Regulatory Commission (NRC) monitors, analyzes and feeds back information on human performance. Review of detailed human performance findings and trends observed in 37 operating events identified through the Accident Sequence Precursor (ASP) program served as the sample of operating experience to which the ROP was compared. All events reviewed had a conditional core damage probability of 1.0E-5 or greater and indicated the influence of human performance. Reviews also considered Individual Plant Examinations (IPEs) and Augmented Inspection Team (AIT) reports. These reviews were then compared to ROP source materials. The ROP source documents included SECY-99-007/007A, SECY-00-0049, NRC manual chapters and inspection procedures, inspection and supplementary inspection reports, plant issues matrices (PIMs), risk-informed inspection notebooks, and the Significance Determination Process (SDP) for Operator Requalification. Insights regarding the characterization of human performance in the ROP are presented.

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

human performance, human reliability, risk, risk contributors, reactor oversight process

13 AVAILABILITY STATEMENT

unlimited

14 SECURITY CLASSIFICATION

(This Page)

unclassified

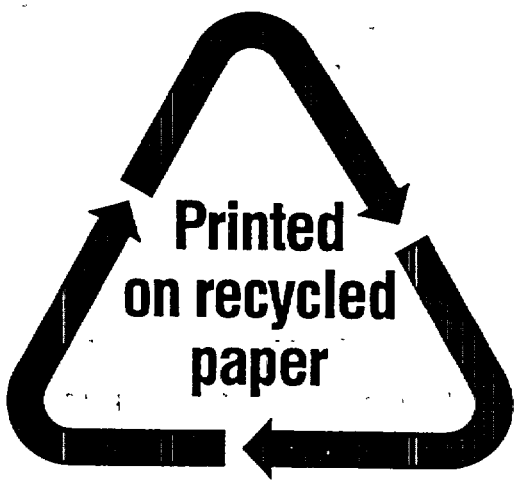
(This Report)

unclassified

15. NUMBER OF PAGES

16 PRICE

NRC FORM 335 (2-89)



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300