Transformer Failure and Common-Mode Loss of Instrument Power at Nine Mile Point Unit 2 on August 13, 1991

Received by OSTI
NOV 12 1991

U.S. Nuclear Regulatory Commission

NUREG--1455

TI92 002691

Transformer Failure and Common-Mode Loss of Instrument Power at Nine Mile Point Unit 2 on August 13, 1991

Manuscript Completed: October 1991
Date Published: October 1991

U.S. Nuclear Regulatory Commission
Washington, DC 20555

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

ypz

ABSTRACT

On August 13, 1991, at Nine Mile Point Unit 2 nuclear power plant, located near Scriba, New York, on Lake Ontario, the main transformer experienced an internal failure that resulted in degraded voltage which caused the simultaneous loss of five uninterruptible power supplies, which in turn caused the loss of several nonsafety systems, including reactor control rod position indication, some reactor power and water indication, control room annunciators, the plant communications system, the plant process computer, and lighting at some locations. The reactor was subsequently brought to a safe shutdown. Following this event, the U.S. Nuclear Regulatory Commission dispatched an Incident Investigation Team to the site to determine what happened, to identify the probable causes, and to make appropriate findings and conclusions. This report describes the incident, the methodology used by the team in its investigation, and presents the team's findings and conclusions.

TABLE OF CONTENTS

Abstract	iii
List of Figures and Tables	ix
Acronyms	xiii
The NRC Team for the Nine Mile Point Unit 2 Transformer Failure and Common-mode Loss of Instrument Power Event on August 13, 1991	xvii
Acknowledgement	xviii
 1 EXECUTIVE SUMMARY	 1-1
2 DESCRIPTION OF FACT-FINDING EFFORTS	
2.1 General Approach	2-1
2.2 Interviews and Meetings	2-1
2.3 Reconstruction of Event	2-1
2.4 Equipment Performance	2-2
2.5 Human Performance	2-2
2.6 Quarantined Equipment and Troubleshooting Procedures	2-3
3 NARRATIVE OF INCIDENT	
3.1 Plant Status Before the Event	3-1
3.2 Loss of Main Station Transformer and Loss of the UPSs	3-1
3.3 Initial Operator Post-Scram Actions	3-3
3.4 Difficulty in Controlling Reactor Vessel Water Level and Pressure	3-5
3.5 Restoration of the Uninterruptable Power Supplies and Recovery Operations	3-6
3.6 Continued Recovery and Approach to Cold Shutdown	3-7
3.7 Event Sequence and Causal Factor Diagrams	3-9
3.8 Graphical Representation of Event	3-13
4 SYSTEM DESCRIPTION, RESPONSES, AND EVALUATION	4-1
4.1 Transformer Fault	4-1
4.2 Electrical Distribution System	4-4

4.2.1	System Overview	4-4
4.2.2	System Response	4-7
4.3	Uninterruptable Power Supplies (UPSS)	4-10
4.3.1	General Characteristics of UPSs	4-10
4.3.2	Description of the 75 kVA 1-Series UPSs	4-10
4.3.3	Post-Event Testing for the 75 kVA 1-Series UPS	4-14
4.3.4	Principal Contributing Factors for Simultaneous Loss of Power Output from the 75 kVA 1-Series UPS	4-17
4.3.5	Pre-Event Maintenance Documentation and Activities for the 75 kVA 1-Series UPS Units	4-17
4.3.6	Post Event Corrective Actions for the 75 kVA 1-Series UPS	4-18
4.3.7	Description of Safety-Related 2-Series UPSs	4-19
4.3.8	Other Potential Causes and Anomalies Investigated	4-20
4.4	Major Uninterruptible Power Supply Loads	4-22
4.5	Instrumentation and Controls	4-28
4.5.1	Control Rod Position Indication and Neutron Monitoring	4-28
4.5.2	Other Balance of Plant Instrumentation	4-33
4.5.3	Safety-Related and Post-Accident Monitoring Instrumentation	4-35
4.6	Condensate and Feedwater Systems	4-36
4.7	Other Systems	4-38
4.7.1	Plant Lighting Systems	4-39
4.7.2	Reactor Core Isolation Cooling System	4-39
4.7.3	Reactor Water Cleanup System	4-41
4.7.4	Residual Heat Removal System	4-41
4.8	Time of Reactor Scram	4-42
5	HUMAN PERFORMANCE	5-1
5.1	Background to Licensee Procedures	5-2
5.2	Initial Operator Response	5-3
5.3	Assessment of Operator Actions	5-7
5.4	Emergency Operating Procedures Training and Other Related Training	5-10
5.4.1	Emergency Operating Procedure Training	5-10
5.4.2	Training on the Uninterruptible Power Supplies	5-12
5.4.3	Simulator Training	5-12
5.5	Command, Control, Teamwork, and Other Issues	5-13
5.6	Other Facility Operating and Event-Based Procedures and Implementation	5-14

5.6.1	Scram Procedure	5-14
5.6.2	Loss of Annunicator Procedure	5-15
5.6.3	Uninterruptible Power Supply Procedures	5-15
5.6.4	Condensate Booster Pumps Operating Procedure	5-16
5.6.5	Use of Damage Control Procedures	5-16
5.6.6	Reactor Core Isolation Cooling Procedure	5-17
5.7	Man-Machine Interface	5-17
6	INCIDENT PRECURSORS	6-1
6.1	Industry Experience with Uninterruptible Power Supply Failures	6-1
6.1.1	Nuclear Plant Reliability Data System Information	6-1
6.1.2	Licensee Event Report Data	6-2
6.1.3	Previous Generic Reports and Documentation of UPS Failures	6-2
6.2	Nine Mile Point Unit 2 Precursors to the August 13, 1991 UPS Failure	6-6
6.2.1	February 1990 Event	6-6
6.2.2	April 1989 Event (LER 89-14)	6-7
6.2.3	NMP-2 UPS Reports to NPRDS	6-7
6.2.4	Review of UPS Work Orders	6-8
6.3	Industry Experience with Transformer Failures	6-8
6.4	Industry and NMP-2 Experience with Overfilling Reactor Vessels	6-9
6.4.1	Licensee Event Report 86-020	6-9
6.4.2	Licensee Event Report 88-001	6-10
6.4.3	Summary of NMP-2 Reactor Overfill Events	6-10
6.4.4	Industry Reactor Overfill Events	6-10
7	REGULATORY REQUIREMENTS	7-1
7.1	Regulatory Classification of Equipment at Nuclear Power Plants	7-2
7.2	Licensee and NRC Staff Actions in Response to Generic Letter No. 83-28	7-5
7.3	NRC Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power Supplies During Operation"	7-7
7.4	Licensee and NRC Staff Actions in Response to Regulatory Guide 1.97	7-7
8	FINDINGS AND CONCLUSIONS	8-1
8.1	Safety Significance of the Event	8-1
8.2	Operator Coping With the Event	8-1

8.3	Transformer	8-2
8.4	Loss of Uninterruptible Power Supplies	8-3
8.5	Instrumentation and Emergency Operating Procedure Integration ..	8-3
8.6	Emergency Operating Procedures Beneficial to Operators	8-4
8.7	Stabilizing Reactor Pressure	8-4
8.8	Scram Procedure Did Not Complement the Emergency Procedures ..	8-5
8.9	Lack of Recovery Procedures at Nine Mile Point Unit 2	8-5
8.10	Condensate Booster Pump Injections at Nine Mile Point Unit 2	8-6
8.11	NRC Expectations on the Treatment of the Balance of Plant Equipment	8-6

APPENDICES

A:	Incident Investigation Team Charter	A-1
	Memorandum from James M. Taylor, Executive Director for Operations, to the Commission Transmitting the Charter for the INVESTIGATION OF AUGUST 13, 1991, EVENT AT NINE MILE POINT, UNIT 2 NUCLEAR POWER PLANT, INVOLVING REACTOR TRIP WITH LOSS OF CONTROL ROOM ANNUNCIATORS AND PARTIAL LOSS OF PLANT INSTRUMENTATION	
B:	IE Bulletin No. 79-27, LOSS OF NON-CLASS 1E INSTRUMENTATION AND CONTROL POWER SYSTEM BUS DURING OPERATION	B-1
C:	Generic Letter 83-28, REQUIRED ACTIONS BASED ON GENERIC IMPLICATIONS OF SALEM ATWS EVENT	C-1

LIST OF FIGURES AND TABLES

Figure	Page
1.1	Nine Mile Point aerial view of units 1 and 2 1-6
3.1	Integrated plant response and operator actions during the first minute of the event 3-11
3.2	Plant response and operator actions during the first half hour of the event 3-12
3.3	Division 1 post-accident monitor (PAM) during initial part of the transient 3-23
3.4	Division 2 post-accident monitor (PAM) during initial part of the transient 3-24
3.5	Division 1 post-accident monitor (PAM) reactor vessel pressure and water level 3-25
3.6	Division 2 post-accident monitor (PAM) reactor vessel pressure and water level 3-26
3.7	Safety relief valves tail pipe temperature, chart motion 1" per hour 3-27
3.8	Reactor vessel water levels in inches 3-28
3.9	Dry temperature - chart speed (1 inch/hour) 3-29
3.10	Narrow and upset range reactor vessel water level 3-30
4.1	Nine Mile Point unit 2 transformer yard 4-43
4.2	Nine Mile Point Unit 2 main stepup transformers and isolated phase bus (IPB) 4-44
4.3	AC onsite power system 4-45
4.4	Offsite power system 4-46
4.5	Simplified protective relaying sketch 4-47
4.6	2MTX-XMIB tank bulging 4-48
4.7	Oil cooler piping flange 4-49
4.8	2MTX-XMIB failed windings 4-50
4.9	Low voltage flashover point phase to phase 4-51
4.10	2MTX-XMIB high voltage tap changers 4-52
4.11	UPS power supply oneline 4-53
4.12	Voltage and current waveforms — 345 kV system 4-54
4.13	Voltage and current waveforms — 115 kV system and RTXA 4-55
4.14	Voltage and current waveforms — 115 kV system and RTXB 4-56
4.15	Frontal view of a 75-kVA 1-series UPS unit 4-57
4.16	Simplified electrical single line diagram for a 75 kVA 1-series UPS unit 4-58
4.17	Card cage for 75-kVA 1-series UPS unit 4-59
4.18	Display panel for 75-kVA 1-series UPS unit 4-60

4.19	Simplified diagram for UPS control logic power supply	4-61
4.20	Simplified electrical single line diagram for safety-related 25 kVA 2-series UPS unit	4-62
4.21	Simplified block diagram for safety-related 25-kVA 2-series UPS unit	4-63
4.22	Reactor manual control system	4-64
4.23	Rod worth minimizer indication after a scram with power available	4-65
4.24	Nine Mile Point unit 2 control room layout	4-66
4.25	IRM/APRM recorder-IRM/APRM/RBM recorder indicating 100% as if UPS lost	4-67
4.26	Back panel 608 APRM status	4-68
4.27	Gaitronics paging unit	4-69
4.28	Post-accident monitoring (PAM) for reactor pressure and level	4-70
4.29	Condensate and feedwater systems (simplified)	4-71
4.30	Reactor core isolation cooling system (simplified)	4-72
4.31	Reactor water cleanup system	4-73
4.32	Residual heat removal system	4-74
5.1	RPV control emergency operating procedures annotated by incident investigation team (reduced from original size)	5-21
5.2	C5 level/power control leg of emergency operating procedures annotated by incident investigation team (reduced from original size)	5-22
5.3	Full core display, rod sequence control, and rod worth minimizer after UPS loss	5-23
5.4	Full core display indicating lights on panel 603 (partial)	5-24
5.5	Panel 603 indicating full power operation (before loss of UPS)	5-25
5.6	Panel 603 after loss of UPS	5-26
5.7	Control room following loss of UPS (generally showing lost instrumentation)	5-27
5.8	Post-accident monitoring (PAM) reactor pressure and level (one of two PAM recorders)	5-28
5.9	Alternate rod insertion (ARI) indication that initiation has occurred	5-29
5.10	Back panel 608 LPRM status	5-30
5.11	RCIC controls	5-31
5.12	RPV control entry conditions of emergency operating procedures	5-32
5.13	RPV control for water level (RL) leg of emergency operating procedures	5-33
5.14	RPV control for reactor pressure (RP) leg of emergency operating procedures	5-34
5.15	RPV control for reactor power (RQ) leg of emergency operating procedures	5-35
5.16	C5 level/power control normal level leg of emergency operating procedures	5-36

Table	Page
2.1 Interviews and meetings conducted by the NMP-2 Incident Investigation Team	2-4
3.1 Chronological Sequence of Events	3-15
4.1 Electrical distribution system input power buses for the UPS units	4-6
4.2 Uninterruptible power supplies for the electrical design at NMP Unit 2	4-11
4.3 Individual no-load battery pack recorded voltage for UPS 1C	4-15
4.4 Individual no-load battery pack recorded voltage for UPS 1D	4-16
4.5 Internal no-load recorded voltage for the three positive and three negative battery packs	4-16
4.6 Major loads on uninterruptible power supply 1A	4-24
4.7 Major loads on uninterruptible power supply 1B	4-25
4.8 Major loads on uninterruptible power supply 1C, 1D, and 1G	4-27
4.9 Control rod indicators	4-31
4.10 Neutron flux monitors indicators	4-32
5.1 Man-machine interface following loss of UPS power output	5-18

ACRONYMS

ac	alternating current
ADS	automatic depressurization system
AEOD	Office for Analysis and Evaluation of Operational Data (NRC)
AOV	air operated valve
APRM	average power range monitor
ARI	alternate rod insertion
ATWS	anticipated transient with scram
BOP	balance of plant
BWR	boiling water reactor
BWROG	BWR Owners' Group
CB	circuit breaker
cps	counts per second
cps	cycles per second
CRAM	control rod drive mechanism
CRD	control rod drive
CSO	Chief Shift Operator
dc	direct current
DMM	digital memory module
DRMS	digital radiation monitoring system
EAL	emergency action level
EAP	emergency action procedure
ECCS	emergency core cooling system
ED	Emergency Director
EOF	emergency operating facility
EOP	emergency operating procedures
EPG	emergency procedure guidelines
ERF	emergency response facility
F	Fahrenheit
FE	flow element
FMEA	failure modes, effects and analysis
FO	fail open
FV	flow valve
FWS	feed water system
GE	General Electric Corporation
GEMS	gaseous effluent monitoring system
GETARS	GE transient analysis recorder system
gpm	gallons per minute

IE	Office of Inspection and Enforcement (former NRC Office)
IEEE	Institute of Electrical and Electronics Engineers
IIT	Incident Investigation Team
IN	Information Notice
INPO	Institute of Nuclear Power Operations
IRM	intermediate range monitor
kV	kilovolt
kVA	kilovolt Ampere
LER	licensee event report
LOCA	loss of coolant accident
LP	low pressure
LPCI	loss pressure coolant injection
LPRM	local power range monitor
LPSI	low pressure injection system
LV	level valve
LWS	liquid rad waste system
MDV	motor operated valve
MOG	motor operated Gates valve
MOV	motor-operated valve
ms	milliseconds
MWe	megawatt electrical
MWt	megawatt thermal
NAO	Nuclear Auxiliary Operator
NMP-2	Nine Mile Point Unit 2
NPRDS	Nuclear Plant Reliability Data System
NR	narrow range
NRC	Nuclear Regulatory Commission
ODI	operations department instructions
OV/UV	overvoltage/undervoltage
PAM	post-accident monitor
PMS	plant monitoring system/plant process computer
PASS	post-accident sampling system
PPC	plant process computer
PSIG	pounds per square inch gravity
PSTG	Plant-specific Technical Guidelines
PWR	power (on equipment labels)
RAT	reserve auxiliary transformer
RCIC	reactor core isolation cooling
RCS	reactor coolant system
RDCS	rod drive control system

RF	radio frequency
RHR	residual heat removal
RHS	residual heat removal system
RL	reactor level
RP	reactor pressure
RPIS	rod position indication system
RPS	reactor protection system
RPV	reactor pressure vessel
RQ	reactor power
RSCS	rod sequence control system
RWCU	reactor water cleanup
RWM	rod worth minimizer
SAE	site area emergency
SCR	silicon control rectifier
SCSS	sequence coding and search system
SEPC	Shift Emergency Planning Coordinator
SER	Safety Evaluation Report
SLC	standby liquid control
SPDS	safety parameter display system
SRM	source range monitor
SRV	safety relief valve
SSS	Station Shift Supervisor
STA	Shift Technical Advisor
TAF	top of active fuel
TMI	Three Mile Island
TS	technical specifications
TSC	technical support center
UAT	unit auxiliary transformer
UPS	uninterruptible power supply

THE TEAM MEMBERS

Members of the NRC Incident Investigation Team for the Nine Mile Point Unit 2 transformer failure and common-mode loss of instrument power event on August 13, 1991, are as follows:

Jack E. Rosenthal, Team Leader
Michael J. Jordan, Assistant Team Leader
Frank S. Ashe
Richard J. Conte
Jose G. Ibarra
Walton L. Jensen, Jr.
John V. Kauffman
M. Marcia Karabelnikoff, Administrative Coordinator
Thomas J. Pohida

INDUSTRY REPRESENTATION

In order to provide industry perspective, expert knowledge of plant hardware and practices, and to facilitate the feedback of factual information regarding the event to the industry for the self-initiation of potential preventive and/or corrective actions, two industry representatives served with the Incident Investigation Team.

William J. Vatter, Institute of Nuclear Power Operations (INPO),
Team Member
James E. Stoner, Jr., INPO Consultant (Duke Power Company)

Technical Editor

Walter E. Oliu

ACKNOWLEDGEMENT

The NRC Incident Investigation Team for the Nine Mile Point Unit 2 event on August 13, 1991, wishes to acknowledge the technical assistance provided by the following NRC staff member:

Steven A. Arndt, Technical Assistant
U.S. Nuclear Regulatory Commission, Office for Analysis and Evaluation of
Operational Data

1 EXECUTIVE SUMMARY

Shortly before shift change on the morning of August 13, 1991, an internal failure in the main transformer at the Nine Mile Point Nuclear Power Plant, Unit 2, caused a turbine trip and reactor scram (i.e., automatic reactor shutdown). During the fraction of a second before automatic protective features isolated the transformer, the fault caused depressed voltages on the transmission system and on the in-plant electrical distribution system. Although of very short duration, the degraded voltage resulted in a simultaneous common-mode loss of five "uninterruptible" power supplies that powered important control room instrumentation and other plant equipment. Internal deficiencies, common to all five power supplies but unknown to the plant staff, had made the power supplies susceptible to failure initiated by degraded voltage.

Automatic reactor protection systems, including the scram, functioned properly. All necessary engineered safety features were available and used as needed. However, control rod position indication was lost, and the operators took conservative action in accordance with their procedures as if there had been a failure to scram. The difficulty experienced by the operators because of the loss of many normally available plant status indications and equipment underscored the importance of the lost power supplies.

The Nine Mile Point Nuclear Power Plant is located on the south shore of Lake Ontario, about 8 miles east of Oswego, New York (Figure 1.1). Unit 2 is a 1080-MWe (net) General Electric boiling water reactor, series 5 (BWR-5), equipped with a Mark II pressure-suppression containment structure. The utility received a full-power operating license for Unit 2 in July 1987. Unit 1, adjacent to Unit 2, is an older design with a separate control room, and its operation was not affected by the event. The plant is operated by Niagara Mohawk Power Corporation (the licensee).

Within each uninterruptible power supply (UPS) that failed, control logic had functioned in response to the degraded voltage causing the UPS input and output power circuit breakers to open. All the equipment powered from the five UPSs was consequently lost. The lost equipment included the following:

- all indications of reactor control rod position, resulting in the operators' inability to verify that the reactor would remain shut down
- condensate and feedwater system controls, resulting in main feedwater pump trips and loss of normal feedwater to the reactor
- virtually all control room annunciators (alarms), hampering the operators' ability to monitor post-scram operation of the plant
- both the in-plant radios and the page telephone communications systems, limiting control room communications with in-plant personnel

- control room indications of plant fire alarms, requiring local monitoring of fire alarm panels
- almost all plant computers that perform monitoring, alarm, protection, and data recording functions, reducing the operators' ability to monitor plant status, disabling some minor automatic functions, and making reconstruction of the event difficult
- multiple control systems, resulting in a loss of normal containment space cooling and requiring that operators divert some attention to monitoring containment temperature
- many other parameter displays on the main control board, limiting the operators' ability to monitor plant conditions, particularly balance-of-plant (e.g., turbine; feedwater) equipment
- the safety parameter display system, removing an aid to operators for analyzing plant conditions, and reducing information that was available in Unit 2's technical support center
- some plant lighting that posed a personnel safety hazard but did not significantly affect plant personnel

Control room operators responded to the loss of feedwater by starting the steam-turbine-powered reactor core isolation cooling system (RCIC) pump; and, the operators used applicable emergency operating procedures. The reactor began to depressurize due to the combined effects of cold water being sprayed into the reactor by the RCIC system and steam being drawn from the reactor by turbine building equipment and the RCIC pump turbine. Although the main feedwater pumps had tripped shortly after the start of the event, two condensate booster pumps remained operating. Valves remained open in the flow path from the condensate booster pumps through the idle feedwater pumps to the reactor. However, water did not immediately flow from this source because the reactor pressure was higher than the condensate booster pump discharge pressure.

As the reactor depressurized below the discharge pressure of the condensate booster pumps, a large uncontrolled volume of cold water was injected into the reactor vessel. Operators recognized the situation, and stopped the condensate booster pumps before the injection had an adverse affect on the plant. However, in the very unlikely event that there had been an actual failure to completely scram the reactor (i.e., an anticipated transient without scram), the injection of cold water and accompanying positive reactivity addition could have resulted in significant consequences. When the cold water was injected, the operators did not know the position of any of the control rods because of the lost rod position indicating equipment, so they were proceeding as if a partial failure to scram had occurred.

The station shift supervisor (SSS) assumed the emergency director's responsibilities and declared a site-area emergency a few minutes after the event began. This emergency declaration was correctly based on a loss of important instrumentation, including

annunciators, combined with a reactor transient. The notification of appropriate local, State, and Federal emergency response organizations followed.

During the first minutes of the event, the control room operators were occupied with many tasks. The assistant SSS assumed the role of shift technical advisor. Within a few minutes, the SSS was filling the roles of both control room supervisor and emergency director. The emergency director's responsibilities, lost instrumentation, efforts to restore electrical power, concern over control rod positions, and other demands placed a heavy burden on the SSS.

Meanwhile, control room operators diagnosed the cause of their lost instrumentation and other important equipment, and dispatched field operators to inspect the UPS and to restore power. When they recognized that the UPS had tripped without transferring loads to alternate power, many of the operators at the UPSs did not know how to proceed. Procedures had not been developed to address the restoration of power following loss of a UPS, but at least one of the operators had sufficient understanding of the equipment to determine what was needed. Power was restored to the UPS loads a half hour after the event began, and operators subsequently verified that all control rods were completely inserted into the reactor core.

Following restoration of the UPS-supplied loads, the event proceeded as a relatively normal plant shutdown. Some operational problems were encountered and they are discussed in appropriate sections of this report. Cold shutdown was achieved that evening at 6:46 p.m., and the site-area emergency was terminated at 7:43 p.m. A detailed chronology of the event is presented in Section 3 of this report.

The Nuclear Regulatory Commission (NRC) initially dispatched a seven-member augmented inspection team (AIT) on August 13, 1991, to investigate the event. However, because of the apparent potential safety significance of the event, and to ensure that any generic technical and operational implications were understood, the NRC Executive Director for Operations (EDO) upgraded this activity to an Incident Investigation Team (the team) on August 15, 1991. The team was formed in conformance with the NRC incident investigation program. (Appendix A contains the EDO memorandum dispatching the team and the team charter.) The team, which included two industry representatives, was selected because of its broad experience in event analysis, with individual members having specific knowledge and experience in electrical power systems, including large transformers and uninterruptable power supplies, instrumentation and controls, boiling water reactor systems and operation, and human performance. The team was directed to determine what happened, identify the probable causes, and make appropriate findings and conclusions. This report documents the results of the team's efforts.

This event did not pose a threat to plant safety, because the scram functioned properly to shut down the reactor. The significance of the event lies in the challenge that it presented to the operators and the potential that severe challenges and resultant stress have to cause errors of omission or commission. The event is also significant because of the simultaneous failure and common-mode vulnerability of the multiple UPSs.

The team found that the event was caused and its course shaped by several factors. Although the transformer failure was the initiating event, it should not be considered a cause in that transformer failure is an anticipated event for which nuclear power plants are designed to safely respond. However, the simultaneous loss of the five UPS was unexpected and presented unique challenges to both equipment and personnel.

Two factors can be considered to be the direct causes of the UPS loss. These are (1) a design deficiency internal to each UPS, and (2) failure of the plant staff to perform appropriate preventive maintenance. Within each UPS there is a control logic unit that is essential to operation of the UPS units. The UPSs were lost because the power for these control logic units was provided by a source that was affected by the degraded voltage resulting from the transformer failure. The control logic units can be supplied with backup power from internal batteries; however, these batteries were dead. Had either deficiency been corrected, the UPSs would not have been lost. All five UPS units are an identical design: hence, all were vulnerable to a loss caused by degraded voltage.

The team examined operator performance and associated human factors. In this event, the operators coped with a difficult situation and successfully addressed the problems that they faced. However, they did make some mistakes that were not safety significant because the reactor scrammed as designed. The operators should have prevented the injection of cold water from the condensate booster pumps. The team concluded that no one factor alone caused this problem; rather, the cause should be attributed to a combination of factors that acted synergistically to result in the operators' unawareness of the impending potential problem in time to prevent the injection. These factors included multiple demands for the operators' attention, the physical layout of the control board, procedure problems, and an unwanted reactor depressurization that was difficult to control. Also, corrective actions in response to previous similar uncontrolled condensate booster pump injections at this site have not been effective in preventing a recurrence of the problem.

In its investigation, the team reviewed prior NRC activities and the licensee's response to regulatory communications that relate the loss of the UPS. The team found that the NRC had not presented a clear position to the regulated industry concerning control of equipment configuration and treatment of important balance-of-plant equipment. Nor had the agency performed an integrated review of instrument and control and operator actions. Such a review could have brought increased attention to the importance of control rod position indication and the challenges its inoperability could present to the operators.

Following this executive summary, the report is organized into the following sections:

Section 2 describes the team's fact finding and investigative efforts.

Section 3 presents a chronological narrative of the event, a tabular sequence of events, and sequence and causal factor diagrams of the first half hour of the event.

Section 4 describes systems and equipment pertinent to the event, and provides a discussion and evaluation of the response of plant equipment during the event.

Section 5 discusses human performance aspects of the event, including operator response, procedures, man-machine interface, command and control, communications, personnel, and training.

Section 6 discusses event precursors, including operating experience with UPSs, transformers, and applicable human performance.

Section 7 discusses regulatory requirements applicable to the event and how the regulatory climate during previous years may have affected the event.

Finally, Section 8 presents the team's findings and conclusions and addresses the potential safety significance of the event.

Figure 1.1 Nine Mile Point aerial view of units 1 and 2

2 DESCRIPTION OF FACT-FINDING EFFORTS

2.1 General Approach

The investigative methods used by the Nine Mile Point Unit 2 (NMP-2) Incident Investigation Team (the team) were developed from the experience gained during previous U.S. Nuclear Regulatory Commission (NRC) incident investigations at San Onofre, Davis Besse, Rancho Seco, and Vogtle nuclear power plants and incorporated into NRC's Incident Investigation Manual (NUREG-1303). Operationally significant events are investigated to identify their probable causes and to provide feedback regarding lessons learned from the investigation to the NRC, the industry, and the public. The NMP-2 team collected and evaluated information from a variety of sources to determine the sequence of events and personnel and equipment responses during the event and their causes.

2.2 Interviews and Meetings

The team placed a high priority on interviewing personnel who were directly involved in responding to the event or who had expert knowledge of the plant's design and responses and of plant conditions. The team conducted interviews early in the investigation while the incident was still fresh in the minds of those involved. The team also met with Niagara Mohawk (the licensee) personnel to discuss informational needs and to agree on a methodology for troubleshooting the quarantined equipment. After leaving the site, the team interviewed NRC staff members concerning a number of regulatory issues that had a bearing on the event. In addition, the team interviewed representatives of Exide Electronics, the manufacturer of the uninterruptible power supplies (UPSs) that lost power output during the event, and representatives of Failure Prevention, Inc., who are performing further failure reconstitution analysis on the UPSs under contract to Niagara Mohawk. The team interviewed the Chairman of the Boiling Water Reactor (BWR) Owners' Group Emergency Procedures Guideline Committee to gain information concerning the development of the emergency operating procedures utilized by licensee control room personnel during the event. The list of interviews and meetings conducted by the NMP-2 team is provided in Table 2.1.

2.3 Reconstructing the Event

The team developed the sequence-of-event descriptions in Section 3 of this report from several sources, including the logs of the Station Shift Supervisor (SSS) and the Chief Shift Operator (CSO), notes taken by plant personnel within the control room, post-event statements of plant personnel, and from interviews with those persons involved in the event, including the NRC inspectors on site at the time. The loss of plant computers and balance of plant instrumentation during the event resulted in the loss of much information that would otherwise be available. For example, the main control room clock was powered by the UPSs and could not be used to set the common time for log entries. A battery-operated clock continued to operate in the rear of the control room and was used by the NRC resident inspector and others in the control room to monitor the event. Control room post-accident monitor (PAM) trend charts powered from safety-related sources recorded the

reactor water level and pressure readings throughout the event. Perturbations in pressure and water level were used to confirm equipment start and stop times. Drywell and suppression pool pressure and temperature readings were also recorded by safety-related equipment. However, trend charts of safety valve tailpipe temperatures were powered by the UPSs and stopped. After power was restored, elevated temperature traces indicated that the two safety valves with the lowest setting (1076 psig) had lifted following the turbine trip. Following the restoration of output power from the UPSs, the paper stuck in the recorder for the narrow and upset range reactor vessel water level instruments. After the paper was freed, those water level indications were continuously recorded after 1:10 p.m. on August 13, 1991. The trend recorder charts are discussed in Section 3.8.

2.4 Equipment Performance

The team evaluations in this area centered on the equipment which failed and initiated the event or which complicated the licensee's recovery efforts. The team reviewed the plant's past operating history, including precursor events, and the status of the equipment to assess equipment performance. In the case of the UPSs that lost power output early in the event, the team evaluated the licensee's troubleshooting procedures and witnessed the diagnostic testing. The team also worked closely with licensee and vendor personnel in analyzing the UPS circuitry to determine the cause of the lost power outputs from the five UPSs and reviewed the licensee's maintenance work order records relating to the five UPSs. The team evaluated data from previous surveillance of the failed B phase transformer and from the A and C phase transformers that did not fail. The team performed a detailed evaluation of the equipment loadings for each UPS unit to determine the impact of the losses and to ensure that the source of various plant equipment losses had been identified. Through interviews and examinations of plant wiring diagrams, the team determined the status of lighting conditions throughout the plant following the loss of "essential" and egress lighting. The team identified and investigated operational deficiencies in certain components of systems utilized in the recovery from the event. Problems not directly related to the event were referred to NRC's Region I for final resolution.

2.5 Human Performance

Losses of instrumentation and communications equipment placed burdens on the plant staff in coping with the event. The team evaluated the emergency operating procedures that were used by control room personnel during the event and their associated training material. At the team's request, the licensee simulated the event on the NMP-2 plant simulator to include a step-by-step walkdown through the emergency operating procedures used by the control room staff during the event. The team's evaluations in this area also relied on interviews with plant staff to assess the adequacy of their training and procedures in coping with the event. The team explored the basis of procedural steps with the BWROG Procedure Guidelines Committee Chairman and with NRC personnel who evaluated the generic guidelines from which the NMP-2 emergency operating procedures were derived.

2.6 Quarantined Equipment and Troubleshooting Procedures

On August 15, 1991, NRC Region I issued a Confirmatory Action Letter which described the licensee's commitments resulting from the event, including their responsibilities to control equipment later quarantined by the team. The licensee could act as necessary to control quarantined equipment, to achieve or maintain safe plant conditions, to prevent further equipment degradation, or to perform tests or inspections required by the plant's technical specifications. NRC and the licensee agreed that these actions would be coordinated with the team's leader in advance or, if that was not feasible, that notification would be made as soon as practical. The team provided the initial quarantined equipment list to the licensee on August 16, 1991. The list included the five UPSs which lost output power and those which did not, all plant switchgear equipment, and plant electric distribution equipment, except for division 3 safety-related equipment. Work was permitted on the main transformers, main generator protective relays, and reactor-protection system motor-generator set output electrical protection assemblies. Items were subsequently removed from the quarantine list when the team determined that the equipment was not related to the resolution of safety concerns identified as a result of the event. Otherwise, troubleshooting controls were left in place. The team reviewed and witnessed UPS testing throughout its time on the site. Before the team left the site, all equipment was removed from the quarantine list, including the five UPS.

Table 2.1 Interviews and meetings conducted by the NMP-2 Incident Investigation Team

Date	Time	Meeting/Interview
8/16/91	3:00 p.m.	Entrance Meeting of IIT with NMP-2 personnel
8/16/91	5:00 p.m.	Plant Tour
8/17/91	8:00 a.m.	Simulator Tour
8/17/91	10:25 a.m.	Interview of reactor operator, NMP-2
8/17/91	12:12 p.m.	Interview of station shift supervisor, NMP-2
8/17/91	2:40 p.m.	Interview of assistant station shift supervisor, NMP-2
8/17/91	4:03 p.m.	Interview of auxiliary operator, NMP-2
8/18/91	8:15 a.m.	Information Exchange Meeting between IIT and NMP-2 personnel
8/18/91	2:12 p.m.	Interview of station emergency plant coordinator, NMP-2
8/18/91	3:15 p.m.	Interview of reactor operator, NMP-2
8/19/91	8:28 a.m.	Interview of assistant station shift supervisor, NMP-2
8/19/91	10:22 a.m.	Interview of control room reactor operator, NMP-2
8/19/91	11:45 a.m.	Interview of reactor operator, NMP-2
8/19/91	1:23 p.m.	Interview of auxiliary operator, NMP-2
8/19/91	2:30 p.m.	Interview of chief shift operator, NMP-2
8/19/91	4:05 p.m.	Interview of auxiliary operator, NMP-2
8/20/91	9:30 a.m.	Interview of shift technical advisor, NMP-2
8/20/91	10:15 a.m.	Interview of operations chief shift operator (relief), NMP-2

Table 2.1 Interviews and meetings (cont.)

Date	Time	Meeting/Interview
8/20/91	11:02 a.m.	Interview of auxiliary operator, NMP-2
8/20/91	11:40 a.m.	Interview of auxiliary operator, NMP-2
8/20/91	1:16 p.m.	Interview of general supervisor of electrical maintenance, NMP-2
8/20/91	1:25 p.m.	Interview of reactor operator, NMP-2
8/20/91	2:20 p.m.	Interview of auxiliary operator (relief), NMP-2
8/20/91	3:09 p.m.	Interview of chief electrician, NMP-2
8/20/91	3:10 p.m.	Interview of reactor operator, NMP-2
8/20/91	3:55 p.m.	Interview of reactor operator, NMP-2
8/21/91	10:15 a.m.	Interview of reactor operator, NMP-2
8/21/91	11:14 a.m.	Interview of auxiliary operator, NMP-2
8/21/91	11:58 a.m.	Interview of auxiliary operator, NMP-2
8/21/91	1:35 p.m.	Interview of auxiliary operator, NMP-2
8/21/91	2:45 p.m.	Interview of general supervisor, operations support, NMP-2
8/21/91	3:32 p.m.	Interview of reactor operator, NMP-2
8/21/91	4:25 p.m.	Interview of reactor operator, NMP-2
8/21/91	4:40 p.m.	Interview of electrical maintenance technician, NMP-2
8/22/91	8:22 a.m.	Interview of consulting engineer to licensee, General Electric Industrial Power Systems
8/22/91	9:25 a.m.	Interview of general physics trainer, NMP-2
8/22/91	11:00 a.m.	Interview of senior operations instructor, NMP-2

Table 2.1 Interviews and meetings (cont.)

Date	Time	Meeting/Interview
8/22/91	2:18 p.m.	Interview of system engineer, NMP-2
8/22/91	3:30 p.m.	Interview of four system engineers, NMP-2
8/22/91	3:45 p.m.	Interview of reactor operator, NMP-2
8/22/91	5:00 p.m.	Interview of general supervisor, operations, NMP-2
8/22/91	6:44 p.m.	Interview of reactor operator, NMP-2
8/22/91	6:45 p.m.	Interview of chief, shift operations, NMP-2
8/23/91	7:20 a.m.	Interview of associate senior generation engineer, NMP-2
8/23/91	1:10 p.m.	Interview of electrical design supervisor, NMP-2
8/23/91	2:08 p.m.	Interview of instrumentation and control mechanic, NMP-2
8/24/91	10:10 a.m.	Interview of instrumentation and control superintendent, NMP-2
8/26/91	9:55 a.m.	Interview of plant manager, NMP-2
8/26/91	1:10 p.m.	Interview of general supervisor for mechanical maintenance, NMP-2
8/26/91	2:10 p.m.	Interview of supervisor, reactor engineering, NMP-2
8/26/91	3:20 p.m.	Interview of general supervisor, instrumentation and control, NMP-2
8/26/91	4:00 p.m.	Interview of operations manager, NMP-2
8/27/91	10:20 a.m.	Interview of resident inspector, NMP-2
8/27/91	3:30 p.m.	Exit Meeting, IIT/NMP-2

Table 2.1 Interviews and meetings (cont.)

Date	Time	Meeting/Interview
8/30/91	8:10 a.m.	Interview of Chief, Instrumentation and Controls Branch, NRC
8/30/91	10:06 a.m.	Interview of Chief, Electrical Systems Branch, NRC
8/30/91	12:15 p.m.	Interview of Chief, Human Factors Assessment Branch, NRC
8/30/91	2:05 p.m.	Interview of Chief, Reactor Systems Branch, NRC
8/30/91	4:08 p.m.	Interview of Staff Member, Committee to Review Generic Requirements, NRC
9/01/91	9:30 a.m.	Information Meeting, IIT/NMP-2/Exide Electronics
9/04/91	11:05 a.m.	Interview of Director of the Division of Operational Events Assessment, NRC
9/04/91	3:15 p.m.	Interview of Deputy Director, Division of Safety Issue Resolution, NRC
9/04/91	4:35 p.m.	Interview of Director, Division of Systems Technology, NRC
9/04/91	12:22 p.m.	Telephone interview of Deputy Director for Reactor Safety, NRC Region I
9/07/91	9:10 a.m.	Information Exchange Meeting, IIT/NMP-2/Failure Prevention, Inc.
9/09/91	9:08 a.m.	Telephone interview of Senior Radiation Specialist, NRC Region I
9/09/91	11:04 a.m.	Interview of Chief, Severe Accident Issues Branch, NRC
9/09/91	1:00 p.m.	Interview of Director, Division of Reactor Inspection and Safeguards, NRC

Table 2.1 Interviews and meetings (cont.)

Date	Time	Meeting/Interview
9/09/91	4:04 p.m.	Interview of Division Director, Division of Licensee Performance and Quality Evaluation, NRC
9/11/91	9:15 a.m.	Interview of Director, Office for Analysis and Evaluation of Operational Data, NRC
9/18/91	9:10 a.m.	Telephone interview of initial training supervisor, general supervisor, operations training, requalification training instructor, training manager, supervisor of reactor engineer, operations manager, NMP-2
9/19/91	10:00 a.m.	Telephone interview of Chairman, BWR Owners' Group Emergency Procedures Guideline Committee

3 NARRATIVE OF INCIDENT

This section provides a narrative description of events at Nine Mile Point Unit 2 (NMP-2) on August 13, 1991, and the consequential plant and operator responses. Loss of plant computers and balance of plant instrumentation during the event resulted in the loss of much information that would otherwise be available. The Incident Investigation Team from the U.S. Nuclear Regulatory Commission (NRC) created this narrative, the chronological sequence of events listed in Table 3.1, and the event sequence and causal factor diagrams in Section 3.7 from other sources, including plant operator logs and statements and from interviews with plant personnel and NRC inspectors on site at the time of the event. The sequence of events in Table 3.1 and the sequence and causal information in Figures 3.1 and 3.2 provide a concise reconstruction of the events in this narrative as an aid to the timing of specific actions or occurrences. Control room strip charts powered from safety-related sources were available throughout the event and were used to confirm equipment start and stop times and the basis for operator actions.

3.1 Plant Status Before the Event

On August 13, 1991, at 5:47 a.m., the reactor was operating normally at 100 percent power, providing 1126 MWe. The plant had been operating at essentially full power since February 10, 1991. Electrical lineups were normal. There were no pre-event data indicating that transformer B was subject to failure.

All 10 uninterruptable power supplies (UPSs) were in operation, including UPS 1A, 1B, 1C, 1D and 1G that lost output power during the event. Of the 10 UPS supplying power to plant equipment, two safety-related UPSs and three commercial-grade UPSs were also in operation and continued to operate throughout the event.

3.2 Loss of Main Station Transformer and Loss of the UPSs

At 5:48 a.m., plant personnel heard a loud "pop" as main station output transformer B developed a fault, causing protective relays to actuate and isolate the transformer from the 345-kV transmission grid by opening the 345-kV generator circuit breakers, the main generator exciter field breakers, and the 13.8-kV switchgear circuit breakers. Recorded data shows that the NMP-2 generator circuit breakers located in the 345-kV switchyard isolated the switchyard from the faulted transformer in 6 cycles (0.1 second). The imbalance in current flow through the B transformer actuated protective relays, which sent a trip signal to the main turbine.

Within a fraction of a second, power output from UPS 1A, 1B, 1C, 1D, and 1G was lost. Offsite power to Unit 2's normal buses was restored by a fast transfer from the normal station service transformer to the reserve station service transformer. The inplant electrical distribution system was isolated from the fault in about 0.15 second and was transferred to the 115-kV reserve station service transformer in another 0.05 second. Emergency buses remained powered through the reserve station service transformer from offsite power throughout the event.

Loss of the five UPSs caused loss of front panel indication including reactor control rod position and average power range monitor recorders. Power was also lost to the feedwater and condensate system instrumentation, as well as loss of plant communication equipment, most control room annunciators, computers, balance of plant (BOP) instrumentation, "essential" and egress lighting, and drywell cooling. (Annunciators are alarm lights in the control room, arranged in panels, that alert operators to the status of plant equipment.) Some instrument indications were failed and others were ambiguous. For example, the narrow range water level strip chart recorder was powered by the UPSs and had stopped in place. Narrow range water level indication A was observed failed downscale. Narrow range water level indications B and C correctly showed a level of 185 inches. The control room fire detection display panel lost power. (See Section 4.4.1 for a listing of the UPS-powered equipment that was lost and Tables 4.6, 4.7, and 4.8 for the condition of the nuclear instrumentation.)

Meanwhile, in a fraction of a second, the main turbine trip actuated the automatic scram (shutdown) of the reactor. The reactor coolant recirculation pumps downshifted to slow speed in accordance with design as a result of the turbine trip. The main steam stop and throttle valves closed on turbine trip, isolating steam flow to the turbine and causing reactor pressure to increase. The alternate rod insertion system (ARI) actuated and the post-accident monitor (PAM) chart recorders shifted to high speed on high reactor system pressure (1050 psig). The PAMs record reactor vessel pressure and water level and are powered by safety-related power. The ARI provides backup control rod insertion. Steam pressure increased causing all turbine bypass valves to open to the condenser and the brief opening of 2 of 18 main steam safety relief valves (PSV-128 and PSV-133) at a pressure of approximately 1070 psig. The two safety valves then reclosed in about 22 seconds after closing at 920 psig. These are the main steam safety/relief valves with the lowest pressure setting and are expected to open following a turbine trip from full power. The safety/relief valves discharge to the suppression pool. The initial increase in reactor vessel pressure from the turbine trip caused the indicated reactor vessel water level to decrease immediately to 145 inches on the wide range scale, which is about 159 inches above the core.

Loss of the feedwater and condensate systems' controls caused minimum flow bypass valves to the condenser to fully open at the discharge of the main feedwater pumps, the condensate booster pumps, and the condensate pumps. The condensate demineralizer bypass valve opened, in accordance with design. The feedwater discharge control valves lost control power and failed to throttle closed. The feedwater heater drain pumps, which also pump water to the suction of the main feedwater pumps, tripped by design when the turbine tripped. Low feedwater pump suction pressure caused the standby condensate booster pump to automatically start, which caused another condensate booster pump to trip on low suction pressure. Both operating main feedwater pumps tripped on low suction pressure when the 18-second delay for this trip expired. Before the main feedwater pumps tripped, continued feedwater flow into the reactor through the open feedwater discharge control valves caused a temporary increase in the reactor vessel water level. Pressure decreased as a result of the addition of subcooled water. (See Figures 3.3 and 3.4 for the reactor vessel level and pressure response and Section 4.6 for a complete description of the feedwater and condensate system during the event.) After the main feedwater pumps tripped, water level

in the reactor vessel decreased as a result of steam losses to the condenser and to the auxiliary steam loads. Pressure increased to the turbine bypass control setpoint of 940 psig.

3.3 Initial Operator Post-Scram Actions

The "popping sound" heard by the control room crew was followed by the instantaneous loss of nearly all annunciators and all lights on the full core display (control rod indication). The crew first assumed that there had been some sort of power failure. As they checked the reactor's power level and pressure on the front instrument panel to evaluate plant status, they noticed that the recorders had stopped and that some indicators had failed upscale, some had failed downscale, and some had failed in place. The red and green lights indicating motor operation and valve positions were lit. All the computer screens were black.

Indications were still available for electrical breaker positions, meters, and safety-related instrumentation. Emergency core cooling systems also had power and instrumentation readings. Operators observed that the PAM recorders had switched to fast speed. Operators looked for indications of a reactor scram: The scram solenoid lights on the front panel were out, providing one indication that a scram had occurred. Operators went to the control room panels behind the front panels and observed downscale readings of average power range monitor instrumentation (APRM) and that the linear power range monitors (LPRM) downscale lights were lit. Scram discharge instrument volumes were observed to be full. Operators concluded that the reactor protection system had initiated a scram. The Assistant Station Shift Supervisor recommended that a manual scram be initiated. The Station Shift Supervisor (SSS) concurred with the recommendation and the Chief Shift Operator (CSO) placed the mode switch to shutdown, which gave a backup manual scram signal to the reactor protection system logic about 1 minute into the event. The time of the backup manual scram was later recorded in control room logs by the SSS and the CSO.

Operators began post-scram followup actions. The intermediate range monitors (IRMs) were driven into the core to monitor neutron flux and indication lights were observed to be lit. Operators then manually tripped the operating reactor water cleanup (RWCU) pump in accordance with post-scram procedures.

During the event, the SSS stationed an operator at the safety-related PAM strip chart recorders and requested that he read reactor pressure and water level indications out loud periodically. The data were recorded by the SSS on the control room emergency operating procedure (EOP) charts laying on top of the computer screen panel. The water level was decreasing since the only water flowing into the reactor vessel at this time was from the control rod drive mechanism (CRDM) pumps. The turbine bypass valves modulated open to maintain reactor pressure at 940 psig. (See Figures 3.5 and 3.6 for condensed PAM pressure and water level data.)

About 7 minutes following the scram, operators initiated reactor core isolation cooling (RCIC) as the reactor vessel water level decreased in anticipation of automatic actuation. The RCIC experienced flow, speed, and pressure oscillations while in automatic control and

operators transferred the system to manual control. (See Section 4.7.2.) The minimum water level reached 150 inches, as recorded on the division 2 wide range PAM recorder. The division 1 PAM was reading only about 4 inches higher. After RCIC was initiated, reactor vessel water level began to increase at a rate of about 2 inches per minute. RCIC flow is normally 600 gpm, but in interviews operators reported that the flow was manually increased to 700 gpm. The spray of RCIC water into the reactor vessel steam space, steam admission to the RCIC turbine, and steam flow to auxiliary steam loads caused pressure to begin decreasing at a rate of about 20 psi per minute.

Because reactor vessel water level was less than the entry criterion of 159.3 inches, operators followed emergency operating procedure "RPV Control." (See Section 5.4.) This procedure requires that operators implement the steps of each flowchart path for control of reactor water level (RL), reactor pressure (RP), and reactor power (RQ) simultaneously. Shortly thereafter, operators left the RL flowchart path of "RPV Control" because control rod positions could not be determined (they were subsequently determined to all be fully inserted) and entered contingency procedure "Level/Power Control," EOP-C5. The automatic depressurization system (ADS) was inhibited in accordance with EOP-C5. Residual heat removal system (RHS) loop-A was initiated in the suppression pool cooling mode to remove heat from the RCIC turbine exhaust.

At about 5:55 a.m., auxiliary operators began coming into the control room from the control building to report the partial loss of lighting and to find out what was going on. Based on their knowledge of the electrical system and experience in a previous UPS loss at the plant (see Section 6), operations personnel in the control room almost immediately recognized that a loss of power from the UPSs had likely occurred. Personnel were dispatched to the normal switchgear building room where four of the five UPSs were located. Other operations personnel were sent out to monitor the condition of the plant from local indicators. Since power was lost to the plant communications systems, personnel had to return to the control room to report on their findings. Local indications confirmed reactor vessel pressure and water level readings from the PAMs and verified that the scram air header was vented. Operators returned from the normal switchgear building at about 6 a.m. and reported that the UPSs had tripped. They were then dispatched to restore power to the UPS loads. Since "essential" plant lighting powered by the UPSs was out, the stairways going down to the UPSs location were dark. Operators used flashlights in negotiating these areas or felt their way along the hand rails. The rooms in the switchgear building where the UPSs were located, were lit from normal ac power that had not been lost because of the successful transfer to offsite power through the reserve auxiliary transformer.

At 6 a.m., the licensee declared a site area emergency, following their emergency action procedure EAP-2 for a loss of control room annunciators with a plant transient in progress. The announcement was made by telephone to Nine Mile Point Unit 1, which made the site announcement since the Unit 2 plant paging system was inoperative. State and local authorities and the NRC were then notified. Between 6:30 and 6:40 a.m., the NRC resident inspector entered the control room.

About 15 minutes after the reactor trip, operators drove the source range monitors (SRMs) into core to measure shutdown neutron flux. The SRMs recorded between 5000 and 40,000

counts per second (cps), which indicated that the reactor was subcritical and producing negligible fission power. Although operators knew that the reactor was subcritical, they did not know if the reactor would remain shutdown if it were cooled since cooldown would add reactivity and they did not yet know the position of the control rods.

At this time, about 6:08 a.m., the crew also had a variety of other tasks and concerns. They were maintaining the condenser available as a heat sink. They considered starting the auxiliary boiler for turbine steam seals, began making preparations to start the condenser mechanical vacuum pumps, and shut down the steam jet air ejector to maintain condenser vacuum. They were also dealing with fire detection and annunciation concerns, such as the potential need to implement fire watches. They were also in the process of identifying what instruments were available and whether they were accurate, performing post-scrum actions and accounting for personnel according to the emergency plan while dealing with the loss of communication equipment, assessing the importance of the loss of drywell fans, and implementing other emergency plan actions.

3.4 Difficulty in Controlling Reactor Vessel Water Level and Pressure

At 6:08 a.m., the RCIC system was delivering water to the reactor vessel at approximately the design flow rate of 600 gpm, a flow rate sufficient to gradually increase water level. Reactor vessel pressure was decreasing. The SSS at this point read the EOPs as not allowing depressurization until control rods were verified as fully inserted. (See Section 5.) As pressure decreased, the RCIC operator was given successively lower pressure bands to maintain. (Operators wished to control the reactor pressure to ensure that the technical specifications cooldown limit was not exceeded and to control recriticality potential in the event that some of the control rods were not inserted.) Steam losses to auxiliary steam loads and RCIC flow continued to reduce reactor pressure, even though the rate of RCIC injection was reduced. Figures 3.5 and 3.6 show the response of reactor vessel water level to RCIC injection.

At 6:11 a.m., reactor vessel pressure decreased below the discharge pressure of the condensate booster pumps which had remained running (about 670 psig). The condensate booster pumps began to rapidly inject water. Operators were at first unaware of the booster pump injection since condensate and feedwater flow indication had been powered by the UPSs and were not now functioning. By 6:14 a.m., operators had responded to the increasing water level and decreasing pressure by terminating RCIC flow to the reactor vessel. They attempted to close the main feedwater control valves but were unsuccessful since the valve control is powered from the UPSs. Reactor water level rapidly increased and passed 202.3 inches at about 6:15 a.m., causing steam flow to the RCIC turbine to be automatically stopped. (The PAM charts were indicating off-scale high.) Operators then tripped the condensate booster pumps. Since the operating condensate pumps will not develop sufficient pressure to inject, the only source of water flowing into the reactor was once again from the control rod drive (CRD) pumps and the reactor water level began slowly decreasing towards the normal operating level. At 6:20 a.m., the condensate pumps were secured, except for P1A. At 7:38 a.m., operators started an additional condensate pump to clear high stator temperature in the operating condensate pump. The maximum

water level from the booster pump injection is unknown since the range of the PAM recorders was exceeded and water level instruments with higher range scales had lost power. (The rate of water level increase indicates that the condensate booster pump water was injected at a flow rate that was about 10 times the 600 gpm flow rate from the RCIC pump.) An extrapolation of the water level increase until the time when the booster pumps were tripped indicates that water did not enter the main steam lines. Reactor vessel pressure reached a minimum of 560 psig following the booster pump injection, corresponding to a temperature decrease of 66° F. The technical specification cooldown limit of 100° F in 1 hour was not exceeded.

3.5 Restoration of the Uninterruptable Power Supplies and Recovery Operations

Meanwhile at about 6:05 a.m., upon reaching the room in the switchgear building containing UPS 1A, 1B, 1C and 1D, operators picked up the operating procedure for the electrical distribution system and located the section on the UPSs. However, they found a procedure for startup, not restoration, which they attempted unsuccessfully to use. There was no procedure for restoration of an UPS in the as-found condition. When licensed personnel arrived, one recalled from startup testing performed with the UPS system engineer how to lift the motor operator from the CB-4 circuit breaker to manually close the breaker to the maintenance (alternate) power source. When they restored UPS 1D output, they heard the plant page system resume operation. At this sign of success, they restored the output from UPS 1A, 1B, 1C, and 1G using the same technique. As a result of the restored power, control room charts which had been recording drywell temperatures from multiple sensors began to decrease from maximums of between 165° F to 120° F. The drywell pressure had increased by 0.65 psi over the period of 34 minutes, which corresponds to an average temperature increase of 25° F. Control rod position indication was also restored. Many rods were indicated as not fully in on the rod sequence control system as well as on the full core display, but there was a disparity between the two displays. One rod on the rod worth minimizer had intermittent indication. Operators began comparing the rod sequence control indication with the full core display rod by rod.

With reactor vessel water level decreasing and at about 160 inches on the PAM recorders at 6:30 a.m., operators began procedures to restart a condensate booster pump. They then planned to control condensate flow into the reactor vessel using the high-pressure/low-flow control valves. The SSS directed that the condensate water be injected slowly while they watched the source range monitors since they still did not know that all control rods were in the core and, therefore, could not rule out recriticality resulting from the addition of too much cold water. The procedures, however, called for first shutting the main feedwater pumps' suction valves. The three valves were closed or verified closed as a precaution stemming from previous water damage to relief valve piping downstream of these valves during startup because of water surge with air in the feedwater lines. Operators started the condensate booster pump at about 6:40 a.m.; however, the three closed valves could not be reopened. The differential pressure across the valves was approximately 500 psig. Bypass valves to equalize pressure around these valves could not be opened since they required local operation within the turbine building. Because returning power to the turbine

building radiation monitors from the restored UPSs had caused false high radiation readings, the turbine building had not yet been cleared for entry.

At about 6:41 a.m., water level again decreased below 159.3 inches, which is the entry condition for emergency operating procedure "RPV Control." The reactor vessel pressure was slowly increasing at this time and reached 630 psig. RCIC was not in operation and operations personnel had been closing off auxiliary steam loads. Operators felt that some water was entering the reactor vessel from the condensate booster pumps by means of leakage through the three closed feedwater suction valves. Operators activated the turbine bypass system at about 6:48 a.m. to reduce pressure and thereby increase booster pump flow into the reactor. Reactor vessel water level continued to decrease, however, and reached a minimum level of about 125 inches on the PAM recorders.

Operators continued to evaluate the ambiguous control rod position indication. At 6:45 a.m. they reset the rod drive control system (RDCS). Some still did not show a full-in indication on either the rod sequence control system or the full core display. One rod still showed misposition on the rod worth minimizer. Source range nuclear instrumentation showed continuously decreasing neutron level in the reactor. At this time, the SRMs were indicating about 1000 cps, which indicates no significant fission heating. Working with EOP 6, Attachment 14, "Alternate Control Rod Insertions," operators placed jumper wires within the reactor protection system cabinets, thus permitting the scram signal to be reset. They then reset the scram signal. Commonly, following a scram, some control rods travel slightly past the full-in position switch and, therefore, do not indicate full-in until the scram signal is reset. Resetting the scram signal removes hydraulic pressure from the control rod mechanisms, allowing them to settle to the normal full-in position. At 7 a.m., all control rods were verified to be full-in, permitting operators to leave EOP-C5, "Level/Power Control." All controls went into the core at 5:48 a.m. when the scram occurred.

About 4 minutes earlier, condensate water flow had been established to the reactor via the low flow/low pressure startup line through valve LV-137, which was opened from the control room. Control room recorders indicated that the reactor vessel water level was slowly increasing at an inch every 5 to 10 minutes. By 7:25 a.m., reactor water level exceeded 159.3 inches, a condition permitting operators to leave emergency operating procedure "RPV Control." Operators did not officially discontinue using the emergency operating procedures, however, until that afternoon when the plant was in shutdown cooling. The exact time that operators discontinued using the EOPs was not recorded in operator control room logs.

3.6 Continued Recovery and Approach to Cold Shutdown

Between 7 a.m. and 12 noon operators continued to restore equipment and to start other equipment needed to reach cold shutdown. The plant process computer, which was powered by UPS 1G, had to be restarted. When restart was completed, the control room alarm printer resumed printing data at 7:11 a.m. At about this time, operators restarted the P2B containment structure hydrogen and oxygen sample pump. (This pump is powered from division 2 of safety-related power and should not have been affected by loss of the UPSs.) The redundant division 1 pump P2A operated throughout the event. Operators started the

condenser mechanical vacuum pumps at 7:29 a.m. The auxiliary boiler was started to provide sealing steam for the turbine. The air operator of auxiliary steam supply valve AOV-145 could not keep the valve open and it had to be locally pinned open. (Plant personnel had experienced difficulty in keeping valve AOV-145 open in the past.) The liquid radwaste computer was restored at 7:50 a.m., hence restoring the safety parameter display system (SPDS), which relies on software which runs on the radwaste computer. Operators experienced difficulty in restarting the stack gaseous effluent monitoring system (GEMS) computer and declared it inoperable until it was subsequently restored at 8:47 a.m. Operators also experienced difficulty in placing the main turbine on its turning gear. The turning gear motor tripped on over current after the turbine coasted down. This occurred about 50 minutes after the turbine trip. The turning gear motor continued to trip on overcurrent each time operators tried to engage it to the turbine rotor. (Investigations into the problem were inconclusive, but the turbine was successfully turned about 8 hours after it stopped and the turning gear motor did not trip. The licensee attributes the problem to temporary bowing of the rotor as it cooled.)

The plant technical support center (TSC) was activated at 7:37 a.m. The station manager, who had arrived about one-half hour earlier at the TSC was apprised of conditions, assumed duty as site emergency director from the SSS at 7:38 a.m. Engineering support personnel for the TSC continued to arrive throughout the morning. The Emergency Operating Facility was activated at 8:04 a.m. and the Onsite Support Facility was activated at 8:07 a.m.

When RCIC testable check valve AOV-156 in the injection line to the reactor did not indicate fully shut, at 9:37 a.m., backup isolation valve MOV-126 was closed to ensure containment structure isolation and RCIC was declared inoperable, in accordance with the plant's technical specifications. RCIC check valve position indication had been a problem in the past and had been subject to both corrective maintenance and modification.

About 9:50 a.m., UPS 1C and 1D loads were restored to power from their normal power source inverters. However, UPS 1A and 1B could not be restored and their loads were left connected to the maintenance (alternate ac) source. UPS 1G loads were restored to normal inverter power at about 10:20 a.m. (See Section 4.3.)

At about 10:06 a.m., control room operators discovered elevated safety/relief discharge pipe temperatures on the control room recorder, indicating that two of the valves had lifted at 5:48 a.m. that morning. (The thermocouple on the discharge pipes from these two safety relief valves still indicated elevated temperatures at 6:22 a.m. when power was restored to the control room recorder and indicated which two valves opened. Two reactor vessel safety/relief valves had indications of seat leakage and were scheduled for repair during the refueling outage scheduled for February 1992. (See Figure 3.7.) They then performed the required full cycle operability test required by technical specification 4.6.4 "Suppression Chamber/Drywell Vacuum Breakers, Surveillance Requirements." (See Section 5.3 for a fuller discussion of this issue.)

Containment purge (i.e., filtered exhaust) had isolated on a false high radiation signal generated by a power spike to the containment radiation monitors when UPS power was restored. Containment purge isolation was reset at 10:31 a.m.

To control reactor water chemistry and to help control reactor vessel level, at about 10:55 a.m., operators started reactor water cleanup (RWCU) pump P1B in the full reject mode of 800 gpm. The system tripped on high differential flow and plant personnel reported hearing a water hammer. (See Section 4.7.3 for a complete discussion of RWCU during the event.)

At the time of the reactor scram, the B and C loops of the RHS were tagged out for electrical preventive maintenance. By 8:10 a.m., operations restored the B and C loops to operable status. Early that afternoon, operations personnel were warming the B train in preparation for putting it in service. This involved opening valve MOV-142, thereby allowing heated reactor coolant to drain through the piping and shutdown cooling heat exchanger to the radioactive waste tanks. Because of an electrical switch problem, operators could not control valve MOV-142 from the control room and, therefore, had to control the valve locally. When the drain line through MOV-142 was opened, plant personnel said that they heard a water hammer. A walkdown of the system at about 1:50 p.m. revealed no damage. Subsequent investigation indicates that what plant personnel heard may have been normal sounds as the pipe heated up. At about 3:08 p.m., RHS pump P1B was started in the shutdown cooling mode. Since RWCU was not operating, the RHS drain line to the radioactive waste tanks was again utilized to control reactor vessel water level with flow through valve MOV-142 being controlled locally. Operators experienced difficulty in controlling reactor vessel water level which began to rise as the B-RHS loop water entered the reactor vessel, was heated, and expanded. High reactor vessel water level generated an automatic trip signal of the main feedwater pumps at 3:19 p.m. The main feedwater pumps, however, were already tripped. High reactor vessel water alarms continued until 5 p.m., when draining reactor coolant through MOV-142 and cooldown of the reactor reduced water level sufficiently to clear the high level alarms. Cooldown continued until 6:46 p.m., when the reactor was declared to be in cold shutdown. At 7:43 p.m., the licensee terminated the site area emergency.

3.7 Event Sequence and Causal Factor Diagrams

Event sequence and causal factor diagrams present the time sequence of different occurrences and their cause-effect relationships. They represent the results of the team's analysis and investigative efforts regarding what happened and how it happened. The diagrams graphically depict the information that is presented in other portions of the report. The early part of the event is presented in two diagrams. Figures 3.1 represents the first minute of the event and Figure 3.2 represents the first half hour of the event. The diagrams depict the event from an integrated perspective. The shapes have specific meanings as follows:

- a. Events that happened normally or as expected at a specific point in time are shown in rectangular boxes. Generally, rectangular boxes do not represent problems that need to be corrected, although the occurrence may be undesirable. Sometimes an undesirable occurrence is a natural or expected response to a previous occurrence. For example, in this event problems culminating in a loss of feedwater were natural and expected responses to the

loss of power that occurred when the UPS failed. Therefore, rectangular boxes are used to represent condensate and feedwater occurrences.

- b. Events in diamond boxes represent an occurrence that was not normal or expected in response to a previous occurrence. Typically, these events are either equipment malfunctions or inappropriate personnel actions. These events are shown in diamond shaped boxes to distinguish them from events that were natural or expected. The diamonds point to aspects of the event where corrective action should be identified to prevent recurrence. A diamond box does not necessarily indicate blame or fault. For example, plant personnel could take inappropriate actions due to conditions beyond their control.
- c. Conditions that caused events to occur and/or resulted from events are shown in oval boxes. These conditions, typically not associated with specific points in time, are important to identify the root cause of the problems depicted in diamond boxes.
- d. Arrows connect the boxes to show cause-effect relationships and relative sequence.

Figure 3.1 Integrated plant response and operator actions during the first minute of the event

CHART KEY:

(time, if known)
events that occurred normally or as expected at specific points in time

(time)
events with inappropriate equipment or personnel performance

Conditions that caused and/or resulted from events. Also, cross references to report

Figure 3.2 Plant response and operator actions during the first half hour of the event

CHART KEY:

events that occurred normally or as expected at specific points in time

events with inappropriate equipment or personnel performance

conditions that caused and/or resulted from events. Also, cross references to report.

3.8 Graphical Representation of Event

The loss of plant computers and balance-of-plant instrumentation during the event resulted in the loss of much information that would otherwise be available to the team for this investigation. Control room post-accident monitor (PAM) trend charts, which were powered from divisions 1 and 2 of safety-related power, displayed and recorded reactor water level and pressure. These charts were used to reconstruct the sequence of events. Perturbations in pressure and water level were used to confirm equipment start and stop times and to aid in the evaluation of hardware and human performance. These charts normally travel through the recorder at 0.75 inches per hour. Following a turbine trip sensed by high reactor pressure (1050 psig), the chart speed increases to 4 inches per minute to permit the recording of rapid changes in pressure and water level. Figures 3.3 and 3.4 show the PAM chart traces starting before the event and including about 90 seconds of the transient after the chart speed changed. The charts show the reactor pressure increase when steam flow from the reactor was interrupted by the turbine trip and the resulting decrease in water level.

The reactor scram quickly reduced reactor steam production. The turbine bypass valves and two safety/relief valves opened, terminating the pressure increase. The safety/relief valves remained open for approximately 22 seconds, causing pressure to decrease and water level to increase. When pressure decreased, the turbine bypass valves closed. When the safety/relief valves reclosed, pressure again increased but was controlled by the reopening of the turbine bypass valves at their setpoint of 940 psig. Feedwater flow into the reactor continued, causing water level to increase after a brief drop caused by the increasing pressure. The division 2 PAM chart indicated a water level only 4 inches lower than the division 1 PAM chart throughout the event. The PAM charts plot reactor vessel conditions from the "wide" range instruments (see Figure 3.8). With the PAM charts moving at 4 inches per minute, 20 feet of chart was generated each hour until operators manually returned the charts to slow speed at about 7:36 a.m., thus generating about 36 feet of chart. The team reproduced these charts on a condensed time scale shown in Figures 3.5 and 3.6. These charts show the effect of operator actions to control pressure and water level during the event.

Drywell and suppression pool pressure and temperature were also recorded by safety-related equipment. Figure 3.9 shows the temperature from sensors at three different elevations in the drywell. The trend chart of safety/relief valve discharge pipe temperatures shown in Figure 3.7 was powered by the UPSs and stopped. Points on the chart correspond to numerals for each of the safety/relief valves. Before the event, two safety/relief valves were leaking, as indicated by elevated discharge temperatures. After power was restored, additional elevated temperature traces indicated that the two safety valves with the lowest setting (1076 psig) had lifted following the turbine trip.

Figure 3.10 indicates water level on the "upset" and "narrow" range scales. This recorder was powered by the UPS and stopped. After the restoration of power outputs from the UPSs, reactor water level on the narrow and upset range instruments became available; however, the paper stuck in the recorder so that narrow and upset range level recording was

not available until 1:10 p.m. The "upset" range charts tracked the water level transient beginning about 3:08 p.m., when operators initiated RHS, which continued until 5 p.m., when the high level alarms cleared. Figure 3.8 compares the "upset" range and "narrow" range instruments with the "wide" range instruments plotted on the PAM charts.

Table 3.1 Chronological Sequence of Events

Initial conditions on August 13, 1991

Plant Status

- The reactor was operating normally at 100 percent power (3322 MWt, 1126 MWe).
- Main transformers A, B, C were supplying power to grid.
- Residual heat removal system (RHS) loops B and C were out of service for preventive maintenance. The A-RHS loop was operable.

Electrical

- Electrical lineups were normal. All 10 uninterruptable power supplies (UPSs) were in operation. This includes UPS 1A, 1B, 1C, 1D, and 1G that lost output power during the event, two safety-related UPS, and three commercial grade UPSs that continued to operate.

Reactor Coolant System

- The reactor is a General Electric BWR 5 design.
- The reactor coolant system was normal, with a water level of 184 inches on the narrow range scale and a pressure of 1004 psig. Both recirculation loops were operating.

Reactor Building and Containment Structure

- The containment structure is a General Electric Mark II pressure-suppression design. The drywell temperature and pressure were 111° F and 0.17 psig.
- The suppression pool temperature was 77° F.

Table 3.1 Chronological Sequence of Events (cont.)

Initial conditions on August 13, 1991

Status of Operations Personnel

- Operators were preparing for shift turnover at 6 a.m.
- Two SROs and one RO from the night shift were in the control room. Two additional ROs were in the plant.
- Three auxiliary operators from the night shift were at various locations in the plant.
- Licensed and nonlicensed operators from the day, relief, and extra shifts were arriving.

Table 3.1 Chronological sequence of events

Key events of August 13, 1991	
<u>TIME (EDT)</u>	<u>DESCRIPTION</u>
a.m.	
5:48	<p>Main station output transformer B developed a fault, which caused protective relays to trip the generator and turbine and to scram the reactor. Within a fraction of a second, output power from uninterruptible power supply (UPS) 1A, 1B, 1C, 1D, and 1G was lost. These failures caused the simultaneous loss of the following instruments and equipment:¹</p> <ul style="list-style-type: none"> — control rod position indicator — feedwater and condensate systems control — most control room annunciators and plant-data computers — balance of plant (BOP) instrumentation — plant communications — "essential" and "egress" lighting — drywell cooling <p>In addition, the following related events occurred during the first minute as a result of the transformer fault:</p> <ul style="list-style-type: none"> — Alternate rod insertion and post-accident monitor recorders to fast speed at 1050 psig — Two SRVs lift at 1070 psig. — Reactor coolant recirculation pumps downshift on turbine trip. — Feedwater heater drain pumps trip on turbine trip and condensate booster pump 2C auto starts. — Condensate booster pump 2A tripped on low suction pressure. — Feedwater pumps trip on low suction pressure. — Division 2 hydrogen/oxygen sample pump trips off. — Operators identify indications of automatic scram: scram solenoid lights out, back panel APRMs and LPRMs downscale, scram discharge instrument volumes full.
5:49	<p>Operators turned the mode switch to "shutdown," thus providing a backup manual reactor scram signal.</p>

¹ See Section 4.4 for a discussion of the equipment lost.

Table 3.1 Chronological sequence of events (cont.)

Key events of August 13, 1991	
<u>TIME (EDT)</u>	<u>DESCRIPTION</u>
a.m.	
5:49	Around this time, the IRMs were driven into the core and downscale lights for range 10 were observed to be lit. RWCU pump manually tripped.
5:55	Operators initiated reactor core isolation cooling (RCIC) in response to decreasing reactor vessel water level and in anticipation of automatic action.
5:56	Operators began to follow emergency operating procedure "RPV Control," since reactor vessel water level decreased to the entry criterion of 159.3 inches, and entered contingency procedure "Level/Power Control," since they were unable to verify control rod position. Operators also inhibited the automatic depressurization system as instructed by the procedure. Operators then initiated suppression pool cooling to remove heat added by the RCIC turbine steam exhaust.
6:00	The licensee declared a site area emergency. About then, operators were sent out of the control room to assess the status of the UPS.
6:03	At approximately this time, operators drove source range monitors (SRMs) into the core. The SRMs recorded between 5000 and 40,000 counts per second (cps).
6:08	The licensee began notifying State and local authorities of the site area emergency.
6:11	The condensate booster pumps began to inject into the reactor.
6:12	The NRC was notified of the site area emergency.
6:14	Operators stopped the reactor core isolation cooling (RCIC) flow into the reactor vessel.
6:15	Reactor water level increased beyond Level 8 (202.3 inches) because of condensate booster pump injection. Steam to the RCIC turbine was automatically stopped on high reactor vessel water level and the condensate booster pumps were manually tripped.
6:20	Condensate pumps were secured, except for P1A.
6:22	Operators manually restored electrical output from UPS 1A, 1B, 1C, 1D and 1G at the UPS cabinets from maintenance supplies, whereupon power

Table 3.1 Chronological sequence of events (cont.)

Key events of August 13, 1991	
<u>TIME (EDT)</u>	<u>DESCRIPTION</u>
a.m.	
6:22	was restored to the control room annunciators and balance of plant instrumentation. The plant communications system and drywell cooling also began to function. Upon its restoration, the control rod monitors indicated that multiple rods were not fully in. Containment purge system (Group 9) isolated on a false high radiation alarm as power was restored to containment structure radiation monitors.
6:30	Operators began procedures for starting a condensate booster pump, shutting or verifying closed the main feedwater pumps suction valves (MOV-84 a, b, and c).
6:40	Operators started condensate booster pump P2A to provide water to the reactor vessel; however, three closed feedwater suction valves could not be reopened.
6:45	Operators reset the rod drive control system. Six rods did not show full-in.
6:48	Operators opened the turbine bypass to reduce reactor system pressure.
6:50	Operators placed jumper wires within the reactor protection system to permit the scram to be reset in accordance with EOP 6, Attachment 14, "Alternate Control Rod Insertion."
6:53	Operators reset the scram signal, which equalized pressure within control rod mechanisms allowing the rods to settle to the normal full-in position. (Some rods had traveled incrementally further than the "00" position.)
6:56	Condensate water flow was established to the reactor via low flow/low pressure startup line through level control valve LV-137.
7:00	Operators verified that all control rods were full-in, permitting them to leave contingency procedure EOP-C5, "Level/Power Control."
7:11	The control room alarm printer was restored. The plant process computer, which was powered by UPS 1G, had to be restarted after power was restored. When restart was completed, the control room alarm printer resumed printing data. Operators restarted the P2B containment structure hydrogen and oxygen sample pump.

Table 3.1 Chronological sequence of events (cont.)

Key events of August 13, 1991	
<u>TIME (EDT)</u>	<u>DESCRIPTION</u>
a.m.	
7:25	Reactor water level exceeded 159.3 inches, permitting operators to discontinue using emergency operating procedure "RPV Control," although operators did not actually stop using the procedure until the afternoon when shutdown cooling was in progress.
7:29	Operators started condenser mechanical vacuum pumps. The auxiliary boiler was started to provide turbine sealing steam. The air operator of auxiliary steam supply valve AOV-145 could not keep the valve open; operators had to pin it open manually.
7:32	Operators experienced difficulty in placing the main turbine on its turning gear.
7:38	Operators started an additional condensate pump to clear a high stator temperature in the operating condensate pump. The station manager, who had arrived earlier at the Technical Support Center (TSC), was apprised of conditions, assumed duty as site emergency director, and relieved the station shift supervisor.
7:50	The liquid radwaste computer was restored, which restored the safety parameter display system (SPDS).
7:58	Operators reset hydraulic power units for the coolant recirculation system flow control valves in accordance with procedures.
8:04	The licensee activated the Emergency Operating Facility.
8:05	Operators experienced difficulty in restarting the off-gas stack gaseous effluent monitoring system computer (GEMS) and declared it inoperable.
8:06	Recirculation system flow control valves were fully opened in accordance with procedures. The valves had been automatically throttled on low reactor vessel water level and feedwater pump trip to decrease core flow, and in turn increase void fraction, hence aid in the reactor power reduction. The operators fully opened the valves in preparation for cooldown to provide for uniform mixing.
8:07	The licensee activated the Onsite Support Center.

Table 3.1 Chronological sequence of events (cont.)

Key events of August 13, 1991	
<u>TIME (EDT)</u>	<u>DESCRIPTION</u>
a.m.	
8:10	RHS loops B and C were restored to operability.
8:21	Operators returned the automatic depressurization system inhibit switch to normal in preparation for leaving the emergency operating procedures (EOPs). The jumpers were removed from the reactor protection system.
8:47	The off-gas stack GEMS computer was restored.
9:37	RCIC testable check valve AOV-156 did not indicate that it was fully shut. The backup MOV-126 was therefore closed in accordance with the licensee's plant technical specifications for containment structure isolation. RCIC was declared inoperable in accordance with the licensee's plant technical specifications.
9:50	UPS 1C and 1D were restored to provide normal output power from their inverters. Normal power from UPS 1A and 1B could not be restored, so their loads were left connected to the maintenance source of power.
10:06	Operators determined that two safety/relief valves lifted early in the event and performed the required drywell vacuum breaker operability test.
10:20	UPS 1G was restored to provide normal output power.
10:31	Operators reset the containment purge isolation system.
10:55	To control reactor water chemistry, operators started the reactor water cleanup system in the full-reject mode (800 gpm). Plant personnel reported hearing a water hammer.
10:56	Reactor water cleanup pump P1B tripped on high differential flow and the reactor water cleanup system isolated.
11:58	Operators secured residual heat removal system (RHS) pump P1A to permit stroke testing of valve MOV 40A, which had undergone preventive maintenance prior to the event.

Table 3.1 Chronological sequence of events (cont.)

Key events of August 13, 1991	
<u>TIME (EDT)</u>	<u>DESCRIPTION</u>
p.m.	
1:10	The narrow range and upset range reactor water level trend recorder, which had stuck after power was restored, was manually restarted.
1:50	System engineers walkdown the RHS following a reported water hammer.
2:15	Operators shut condensate demineralizer bypass valve AOV-109 to control condensate system chemistry. The valve had opened automatically early in the event.
3:08	RHS pump P1B was started in the shutdown cooling mode.
3:19	The high reactor vessel water level generated an automatic trip signal of the main feedwater pumps, but they were already tripped. Condensate booster pump P2A was then shut down. An electrical problem with RHS throttle valve MOV-142 controlling coolant flow to the radioactive waste tanks caused difficulty in controlling reactor vessel water level.
3:20	Condensate pump P1A was shut down.
3:28	The control room alarm printer indicated a high water-level condition in the reactor vessel (206 inches narrow range).
5:00	Cooldown of the reactor continued and reactor vessel water level decreased and high-level alarms cleared.
6:07	Main feedwater isolation valves 2FW-MOV21A and 21B were closed.
6:46	The reactor was declared to be in a cold shutdown.
7:42	The licensee terminated the site area emergency.

Section 3

Figure 3.5 Division 1 post-accident monitor (PAM) reactor vessel pressure and water level

Figure 3.6 Division 2 post-accident monitor (PAM) reactor vessel pressure and water level

Figure 3.7 Safety relief valves tail pipe temperature, chart motion 1" per hour

Figure 3.8 Reactor vessel water levels in inches

Figure 3.9 Dry temperature
Chart speed (1 inch/hour)

Increasing Time →

NARROW RANGE WATER LEVEL

UPSET RANGE WATER LEVEL

↑
PAPER STUCK
AND ADVANCED
AT 1:10 PM

Figure 3.10 Narrow and upset range reactor vessel water level

4 SYSTEM DESCRIPTION, RESPONSES, AND EVALUATION

This section provides the team's evaluation of the major systems and support systems that were affected by the transformer fault and the ensuing loss of output power from the uninterruptable power supplies (UPSs). This section also describes and evaluates important systems used during the event. Finally, this section includes an evaluation of the time when the reactor scrammed.

The descriptions and evaluations included in this section follow the sequence of events discussed in Section 3. The discussion begins with the transformer fault and its effect on the plant internal electrical distribution system and continues with the loss of power from the UPSs and its effect on plant recovery activities, including instrumentation and control systems, condensate and feedwater, plant lighting, reactor core isolation cooling (RCIC), reactor water cleanup (RWCU), and residual heat removal (RHS).

4.1 Transformer Fault

On August 13, 1991, at 5:48 a.m., the B phase 345/25-kV unit main stepup transformer at Nine Mile Point Unit 2 failed. Some oil spilled, but no fire occurred and there was minimal external physical damage to ancillary and interfacing equipment. An aerial view of the Nine Mile Point Unit 2 transformer yard is shown in Figure 4.1, and a ground-level picture of the Unit 2 main stepup transformer layout is shown in Figure 4.2.

At the time of the failure, the unit was operating at a generator loading of approximately 1126 MWe, well within the transformer and the generator capability, supplying power to both the 345-kV transmission system (through the 345/25-kV main stepup transformer bank composed of single-phase transformers A, B, and C with D available as an installed spare) and 13.8-kV nonsafety-related electrical station service loads (through the 25/13.8-kV normal station service transformer). Figure 4.3 depicts the onsite power system arrangement. The 4.16-kV safety-related emergency power distribution system was connected to its normal sources of power, which are the 115/13.8/4.16-kV reserve station service transformers located in the transformer yard at the plant. The reserve station service transformers derive their power from 345-kV Scriba switchyard buses A and B through separate 345/115-kV transformers (located at diagonally opposite corners of the Scriba switchyard). The reserve station service transformers normally provide power to the safety-related emergency power distribution system, as well as serving as an alternate source of power for the 13.8-kV normal nonsafety station service electrical distribution system. Figure 4.4 depicts the offsite power system arrangement. At the time of the event, there were no 345-kV transmission system or plant electrical system switching or operational activities being performed, nor were there any unusual weather conditions or other factors which may have caused or precipitated the transformer failure.

The failure was promptly detected by protective relaying, which isolated the failed transformer and automatically transferred the normal station service distribution system to its alternate sources, which are the reserve station service transformers. The protective

relaying operated as designed during this event. The sequence of protective relay operation was not recorded because the relays were not connected to a sequence of events recorder. The protective relaying which actuated during this event is depicted in Figure 4.5 and summarized as follows:

- The main transformer differential relay and its associated lockout and tripping relays trip the main turbine, the unit generator 345-kV circuit breakers at Scriba, the 13.8-kV normal station service switchgear source circuit breakers, and the unit generator exciter circuit breakers.
- The unit protection differential and its associated lockout and tripping relays trip the main turbine, the unit generator 345-kV circuit breakers at Scriba, the 13.8-kV normal station service switchgear source circuit breakers, and the unit generator exciter circuit breakers.
- The transformer fault pressure relay and associated lockout and tripping relays trip the main turbine, the unit generator 345-kV circuit breakers at Scriba, the 13.8-kV normal station service switchgear source circuit breakers, and the unit generator exciter circuit breakers.
- The high voltage neutral-to-ground overcurrent relays and their associated lockout and tripping relays trip the main turbine, the unit generator 345-kV circuit breakers at Scriba, the 13.8-kV normal station service switchgear source circuit breakers, and the unit generator exciter circuit breakers.
- The generator "startup" phase overcurrent instantaneous relays in B and C phases picked up but their output is blocked when the unit is on-line, since this relay circuit is intended to provide protection when Unit 2 is off-line.

Other pertinent relaying that did not operate, per design, is as follows:

- The generator differential relaying which is provided to operate in the event of an internal generator fault did not operate during this event, as would be expected.
- The generator neutral ground overcurrent relay did not operate, but this does not necessarily mean that the low voltage winding did not fault to ground due to the relay response time. In addition, this relay circuit is blocked by the lockout relays which were actuated by the transformer differential relay, the transformer fault pressure relay, and/or the transformer neutral ground overcurrent relays. Therefore, if the low side transformer winding did fault to ground during the event, there would be no indication. It is important to note that even if the low side transformer windings did fault to ground, the amount of ground fault current that could have flowed from the unit generator is limited by the generator neutral ground circuit design to a maximum of 7.5 amperes, which comparatively speaking, is negligible.

The team's inspection of the failed transformer yielded the following observations:

- **The transformer's main tank was bulged on the two sides at the ends of the coil windings, as depicted in Figure 4.6.**
- **The isolated phase bus connecting the generator to the transformer was not damaged, and is shown in Figure 4.2.**
- **None of the transformer bushings were damaged.**
- **Some of the oil cooler piping flange joints were bent and leaking oil, as shown in Figure 4.7.**
- **In-tank inspection of the transformer after the transformer oil was removed revealed:**
 - **some damage to the wooden bus supports, as shown in Figure 4.8,**
 - **arcing damage to a portion of the high voltage and low voltage windings, with minimal copper splatter, as shown in Figure 4.8**
 - **bent low voltage lead busbars as shown in Figure 4.9, and**
 - **minor arcing between the low voltage winding phase leads, as shown in Figure 4.9, with minimal copper splatter. This arcing most likely occurred after the first few cycles because of the magnetic forces and pressure causing movement of the coils, leads, and low voltage busbars, which resulted in the low voltage phase leads coming in close proximity to each other**
 - **no evidence of arcing to the inside of the tank at accessible locations**
 - **no evidence of any damage to either the stationary or movable contacts of the tap changer, as shown in Figure 4.10. The tap changer contacts were clean and showed no evidence of overheating, and the support structure and changer mechanisms did not appear to be mechanically or structurally damaged**
- **The damage to the coils appeared to result from a failure that originated deep within the coils. To further assess the cause of the failure, the coils will have to be removed and disassembled. The damage observed involved multiple turn-to-turn failures of both the high and low voltage windings.**

Relay flags as well as oscillographic voltage and current traces from the 345-kV Scriba switchyard digital data recorder indicate that the fault was initiated by a failure of the high

voltage winding to ground. However, there are several plausible explanations which are compatible with the relay and recorder information gathered.

There is no assurance that the exact cause of the failure can be determined, even if the transformer core and coil assembly are carefully disassembled. However, this is the only course of action which might possibly yield such a determination. The question of what caused the insulation failure also has several possible answers, ranging from manufacturing defects to a latent failure caused by geomagnetically induced currents. The licensee has removed the transformer from the transformer yard, and is planning to return the failed transformer to the manufacturer in order to try to determine the cause of the failure.

The team reviewed the adequacy of the periodic maintenance program that had been followed for the failed transformer with regard to inspection, testing, and preventive maintenance practices, and the acceptability of recently recorded periodic maintenance data. An inspection procedure covering both daily and weekly inspections was being followed by Niagara Mohawk. Daily inspections included recording of transformer winding and oil temperatures, transformer and bushing oil level, gas volume indication, pressure relief device inspection, cooling fan inspection, and oil flow through the oil pumps. Weekly inspections included recording of control cabinet heater status, and control cabinet cleanliness in addition to the daily inspections. Quarterly oil analysis had been last performed at the end of May 1991 in accordance with procedure. The analysis measures dissolved gases in the transformer oil and is an indication of potential problems. The analysis of the May oil sample for the B phase transformer yielded satisfactory results. The refueling outage electrical preventive maintenance procedure had been completed in December 1990. This procedure required transformer annunciator operability testing; oil cooler fan and oil pump operability verification and repair as appropriate; and, control panel electric heater operability verification and repair as appropriate.

The team found that the data available from the recent daily, weekly, quarterly, and refueling maintenance and sampling records did not give any anticipatory indication that a failure of the transformer was imminent.

4.2 Electrical Distribution System

4.2.1 System Overview

The unit generator is connected through an isolated phase bus system to the unit main stepup transformer bank which transforms the voltage from 25-kV on the generator side to 345-kV on the high voltage system side. The unit main stepup transformer bank consists of three single-phase transformers, with a fourth installed as a spare as shown in Figures 4.1 and 4.2. The spare can be readily connected as a substitute for any one of the three transformers normally in service in the event one of them fails. The unit generator connects to the 345-kV Scriba switchyard, which is located 0.5 miles from the plant through a single transmission circuit connected to two 345-kV generator circuit breakers which connect to separate 345-kV buses in the switchyard. A tap off of the 25-kV generator isolated phase bus system connects to the normal station service transformer, which is the source for the

13.8-kV normal station service electrical distribution system when the unit is on-line. The normal station service transformer is a three winding transformer which transforms the voltage from 25-kV on the high voltage winding to 13.8-kV on each of the two low voltage windings. Separate 13.8-kV switchgear circuit breakers connect the two low voltage windings of the normal station service transformer to the two 13.8-kV switchgear units (SWG001 and SWG003) which normally supply power to the station service electrical distribution system. Switchgear units SWG001 and SWG003 are provided with a redundant source of power from separate 115/13.8/4.16-kV reserve station service transformers. These provide power to the 13.8-kV switchgear during plant startup and normal plant shutdown. The five uninterruptable power supply (UPS) units from which output power was lost during the event receive their normal and maintenance (alternate) power from switchgear units SWG001 and SWG003. The 13.8-kV switchgear unit SWG001, through multiple transformers, supplies normal power to UPS 1D, supplies maintenance (alternate) power to UPS 1A and 1C, and serves as a redundant source of normal power to UPS 1A, 1B, and 1G. The 13.8-kV switchgear unit (SWG003), through multiple transformers, supplies normal power to UPS 1A, 1B, 1C, and 1G, and supplies maintenance (alternate) power to UPS 1B, 1D, and 1G. This electrical distribution system alignment is depicted in Figure 4.11 and tabulated in Table 4.1.

The onsite emergency or safety-related power distribution system receives its power from the two 115/13.8/4.16-kV reserve transformers, with each of the two safety trains normally supplied from separate reserve transformers. This was the alignment of the safety-related power distribution system during the event on August 13, 1991.

Table 4.1 Electrical distribution system input power buses for the UPS units

UPS UNIT	NORMAL		SOURCES	MAINTENANCE SOURCE
	600 V NORMAL BUS	600 V REDUNDANT NORMAL BUS		
UPS-1A	US-3 BUS B	US-4 BUS A	600 V BUS	2NJS US-5
UPS-1B	US-3 BUS B	US-4 BUS A		2NJS US-6
UPS-1C	US-3 BUS B	(NONE)		2NJS US-5
UPS-1D	US-3 BUS A	(NONE)		2NJS US-6
UPS-1G	US-3 BUS B	US-4 BUS A		2NJS US-6

4.2.2 System Response

The factual information captured to aid the team in reconstructing the electrical power system parameters immediately before, during, and following the event are oscillograph traces of selected 345-kV and 115-kV line voltage and current waveforms from the 345-kV Scriba switchyard digital data recorder (Figures 4.12, 4.13, and 4.14), recorded as-found protective relay flags, and the post-event as-found state of the electrical distribution system equipment. The 345-kV system is connected to the normal station service transformer through the unit main stepup transformer, and the 115-kV system supplies the reserve station service transformers. There were no recordings of either the in-plant nonsafety or safety-related electrical distribution system voltage or current magnitudes or waveforms during or following the event at either the 13800, 4160, 600, or 208/120-volt ac buses in the plant.

The recorder in the Scriba switchyard continuously records data while maintaining a four-cycle pre-initiation memory. Line 23 connects the Nine Mile Point Unit 2 main stepup transformer to the 345-kV Scriba switchyard. The digital data recorder at the Scriba substation was connected to monitor four points associated with line 23: the C Phase current and line-to-neutral voltage (Figure 4.12, rows 10 and 13), and the main stepup transformer wye-connected high-side winding neutral current and voltage (Figure 4.12, rows 11 and 12). Other pertinent points being monitored include the 345-kV Scriba switchyard bus A phase A, B, and C line voltages (Figure 4.12, rows 1, 2, and 3). The oscillograph traces of the various voltage and current waveforms monitored shows that during the four-cycle period prior to the transformer failure, there were no voltage or current excursions, perturbations, or variations indicating that anything unusual precipitated the transformer failure. The oscillograph trace in Figure 4.12 shows that the fault began manifesting itself (row 11) approximately one-third of a cycle before it became fully established, as evidenced by the sharp B phase voltage degradation (row 2) on the Scriba 345-kV switchyard bus A. The 345-kV line-to-ground current quickly increased from zero to approximately 1300 amperes in approximately one and one-half cycles from the instant the fault began manifesting itself.

In a step function manner, the line voltage on the line 23 C phase decreased from 213-kV to 172.5-kV (81 percent), and the line current increased in the same manner from 1740 amperes to 6100 amperes (350 percent). Similarly, the A and C phase Scriba switchyard bus A line voltages decreased from 210-kV to 180-kV (86 percent), while the B phase decreased from 213-kV to 82.5-kV (39 percent). Thus, it is reasonable to postulate that the line 23 A phase voltage also was approximately the same as the line 23 C phase voltage of 172.5-kV (81 percent) and the line 23 B phase voltage was approximately the same as the B phase voltage on the Scriba switchyard bus A value of 82.5-kV (39 percent).

All the voltages and currents appear to have remained stable and constant at their decreased values, with no variations or perturbations from cycle-to-cycle for the entire six cycles (0.1 second) that the transformer remained connected to the 345-kV system grid before its isolation from the grid by protective relaying action which tripped the two 345-kV generator circuit breakers in the Scriba switchyard. As shown in Figure 4.12, all the monitored voltages and currents restored themselves to values that would be expected after

the 345-kV system grid was isolated from the fault. One noteworthy item is that the C phase voltage on the main stepup transformer decreased to approximately 172-kV during the event and continued to decay slowly after isolation from the 345-kV transmission grid to approximately 123-kV after 40 cycles, and continued to decay to approximately 75-kV during the remaining 60 cycles on the recording because the transformer remains connected to the unit generator. The voltage probably did not reach zero until some 3 to 4 seconds (180 to 240 cycles) after the generator exciter field circuit breaker and turbine trips were initiated coincident with initiation of the 345-kV switchyard generator circuit breaker trip.

Thus, even though the 345-kV system grid was isolated from the failed transformer within some 6 cycles (0.1 second) after the fault occurred, the unit generator continued to feed the fault for some 3 to 4 seconds (180 to 240 cycles) after the fault was established because of the large amount of energy stored in, and the relatively long time constants of, both the generator and its exciter. However, the unit generator did not contribute to the high-side ground fault current since the generator was connected to the low (delta) side of the transformer.

It should be noted that only the 345-kV system grid would have been a source for the 1300 amperes flowing through the high-side neutral ground circuit, and all of the 1300 amperes flowing in this ground circuit would have returned to the 345-kV grid. Unless the low side winding, which is delta connected, also faulted to ground at some time during the event, no current would have flowed from the unit generator to ground. If the low side winding did fault to ground during the event, the maximum amount of current that the unit generator would have provided would have been approximately 7.5 amperes because of the generator neutral grounding design. Likewise, any ground fault current which might have been provided by the unit generator would have returned to the unit generator, and would not have involved any of the electrical distribution system equipment or loads within the plant.

The protective relaying that initiated the isolation of the 345-kV system grid, the turbine, and the generator field excitation, also initiated the isolation of the 13.8-kV normal station service switchgear from the normal station service transformer, which is solidly connected to the generator and to the low side winding of the main stepup transformer. There were no recordings of voltages and currents on the low (generator) side of the main stepup transformer, or on any of the switchgear, buses, or load centers within the plant at any voltage level. Therefore, any postulation of events, voltages, or currents that may have manifested themselves within the plant would be based on extrapolations and judgements based on previous experience.

While the 345-kV switchyard generator circuit breakers isolated the 345-kV system grid from the fault in six cycles, the 13.8-kV switchgear circuit breaker would have been expected to isolate the normal station service switchgear from the fault in approximately nine cycles because of the difference in rated fault interrupting time for the two types of circuit breakers. (The 345-kV circuit breakers have a two-cycle rated interrupting time, while the 13.8-kV circuit breakers have a five-cycle rated interrupting time.) This means that the generator continued to feed the fault and supply normal station service load for a period of approximately nine cycles during the event.

Based on the information available in Figures 4.13 and 14, the 13.8-kV switchgear was successfully transferred to the two 115/13.8/4.16-kV reserve station service transformers approximately 12 cycles after initiation of the event. It then follows that the 13.8-kV switchgear was not connected to any power source for approximately three cycles during the event. Because of the stored energy in the rotating induction motors, when separated from the unit generator, they would behave as induction generators during the approximately three cycles that the nonsafety-related electrical distribution system was not connected to any external power source during the transfer. Hence, the voltage on the plant nonsafety-related electrical distribution system would be expected to be depressed during the approximately nine cycles that it was connected to the unit generator and the faulted system, and would be expected to decay rapidly to zero within some three to six cycles after the system was separated from the unit generator. In this case, the normal station service system was reconnected to the reserve station service transformer within approximately three cycles after isolation from its normal source. As shown in Figures 4.13 and 4.14, the initial current inrush through the reserve station service transformers was approximately 260 percent of the steady-state current recorded 15 cycles following the transfer.

Based on approximations and judgement, the licensee has estimated that the normal station electrical distribution B phase voltage decreased to approximately 50 percent of rated voltage during the approximately nine cycles that the unit generator remained connected to the 13.8-kV normal electrical distribution system. The team agrees that this approximation is reasonable. It should be noted that the five UPS units which failed derived the input power for their control logic from B phase of the normal station service electrical distribution system.

Since the source of power for the 4.16-kV emergency (safety-related) power distribution system is also the 345-kV Scriba switchyard, then it follows that the voltage depressions in the Scriba switchyard would have been reflected directly into the emergency power distribution system and would have been approximately the same as the voltage depressions on the 13.8-kV normal station service electrical distribution system described earlier in this section, but only for the first six cycles of the event. The voltages on the 115-kV buses, supplied from the 345-kV buses, are shown in Figures 4.13 and 14. As would be expected, the emergency (safety-related) power distribution system degraded voltage relays were actuated, as shown by their flags which were dropped, but the degraded condition did not exist long enough for the degraded grid protective relaying circuit timers to time out. The degraded condition on the emergency power distribution system would have lasted for only six cycles, as is shown on Figures 4.13 and 4.14; therefore, the diesel generator start and the offsite source circuit breaker trip signals were not initiated. Hence, the emergency (safety-related) power distribution system degraded voltage protection system operated as designed during this event.

The safety-related UPS systems operated as designed during this event. The power source for the control logic for the safety-related UPS units is the 125-V dc safety-related battery system. The safety-related UPS units were reported to have lost synchronism with the emergency power distribution system during this event because of the voltage depression also experienced by the emergency power distribution system. The UPS units monitor both the frequency and the voltage magnitude of its alternate source as a condition for staying

in synchronism with the maintenance supply. Thus, if either of these variables are outside of their predetermined limits, the UPS unit detects this condition and locks out the maintenance supply as a possible source. In this case, the magnitude of the voltage excursion on the ac maintenance supply was below its design limit and, therefore, these UPS operated as designed.

4.3 Uninterruptible Power Supplies (UPS)

4.3.1 General Characteristics of UPSs

Uninterruptible Power Supplies (UPS) are designed to provide continuous power to important electrical loads should the UPS lose their normal ac input power source. UPSs are designed to preclude the three most common power disturbances which affect the reliable operation of electrical equipment loads: (1) power line noise, (2) power fluctuation, and (3) sudden loss of power. Together, power line noise and voltage fluctuations account for the major percentage of all power-oriented equipment problems and/or malfunctions. The Nine Mile Point Unit 2 (NMP-2) electrical design was implemented with 10 UPS units. Specific features for these units are provided in Table 4.2.

4.3.2 Description of the 75 kVA 1-Series UPSs

Five of 10 UPSs units lost power output when an electrical fault occurred on the B phase main station output stepup transformer. Design specifications for each of these units are identical. Figure 4.15 shows a photograph of the unit. Circuit breakers (CBs) CB-1, CB-2, CB-3, and CB-4 are discussed later in this section and are shown at the bottom front of the unit.

A 600-V ac 3-phase input power source from the in-plant electrical distribution system provides the normal ac input power to the UPS unit (see Figure 4.16). When CB-1 is closed, 600-V ac 3-phase power is applied to the input of an ac to dc converter. This converter, consisting mainly of transformers, SCRs, and filtering interconnecting circuits, provides a regulated dc voltage source output.

This output is the normal power source input to the dc-to-ac inverter. If the 600-V ac source of power is unavailable, the dc power source is provided by a 5100-ampere-hour storage battery. This source of power to the inverter is by way of CB-2 and a blocking diode. The diode prevents the converter from charging the storage battery. Similarly, if the output section of the converter is unavailable, converter circuit elements prevent discharging the storage battery. A separate battery charger maintains the storage battery.

The dc-to-ac inverter, consisting primarily of interconnecting transformers, SCRs, and filtering circuit elements, provides a high quality ac output power source. This is the normal source of power output from an UPS unit and is provided to the critical loads by way of CB-3. The inverter regulates its output voltage to within one percent of a nominal value. An alternate source of UPS power output is a maintenance supply. The term maintenance supply reflects its purpose (i.e., to power the normal UPS loads when maintenance is being performed on these units). It is not equivalent to inverter output.

Table 4.2 Uninterruptible power supplies for the electrical design at NMP Unit 2

UPS	Series*	kVA Rating	Voltage and Phase of Power Output	Safety Related
1A	1	75 kVA	208/120 V ac - 3 Phase	No
1B	1	75 kVA	208/120 V ac - 3 Phase	No
1C	1	75 kVA	208/120 V ac - 3 Phase	No
1D	1	75 kVA	208/120 V ac - 3 Phase	No
1G	1	75 kVA	208/120 V ac - 3 Phase	No
2A	2	25 kVA	120 V ac - Single Phase	Yes
2B	2	25 kVA	120 V ac - Single Phase	Yes
3A	3	10 kVA	120 V ac - Single Phase	No
3B	3	10 kVA	120 V ac - Single Phase	No
1H	1	5 kVA	120 V ac - Single Phase	No

Note: All UPSs kVA ratings are at a power factor of 0.8.

*The five 75-kVA 1-series UPS units were manufactured in 1981 and were placed in service at the site in 1985.

This supply is provided by in-plant electrical distribution buses which are different from those for normal UPS ac input. The maintenance supply (alternate) is applied to the UPS unit by way of a stepdown transformer and a regulator. The regulator is designed to maintain its output voltage within two percent of nominal for a range of input voltages.

When CB-4 is closed and CB-3 is opened, the regulated alternate maintenance supply is the power output for an UPS unit. CB-3 and CB-4 are motor-operated circuit breakers and receive automatic electrical signals from the UPS unit's control logic to appropriately open and close.

UPS Control Logic

The control logic provides automatic electrical signals to the converter, inverter, circuit breakers, and static power transfer switch which are necessary for proper operation of the UPS unit. For conditions which could result in improper UPS operation, severe internal component damage, or destruction to the UPS normal power output source (i.e., the inverter), the control logic provides automatic electrical signals to open CB-1, CB-2, and CB-3, thus isolating the converter and the inverter.

The control logic also provides an electrical signal which permits CB-3, CB-4, and the static power transfer switch to be operated when the UPS power output source is automatically transferred from the inverter to the maintenance supply. This transfer is only permitted if the sine waveform voltage amplitude, frequency, and voltage phase angle differences between the inverter output and the maintenance supply are within pre-determined limits. These limits for the 75 kVA 1-Series units are 10 percent, 0.5 Hz, and 7° for amplitude, frequency, and phase angle, respectively. Electrical signals from the UPS unit's control logic operate the static power transfer switch such that a smooth power transfer of the critical loads from the UPS unit normal power output source (i.e., inverter) to the maintenance supply (alternate) occurs within 4 milliseconds (ms). The static transfer switch and associated control signals are essential for a smooth power transfer since CB-4 requires from 64 to 84 ms to close. A smooth power transfer is required in order to prevent improper operation or damage to sensitive electrical loads powered from the critical bus.

A card cage contains nine printed circuit boards (Figure 4.17). These circuit boards plug into connectors which are attached to the card cage. The connectors are interconnected by wiring on a printed circuit board. The card cage houses the control logic hardware that provides essential electrical signals for an UPS unit. The circuit boards include dual in-line pin integrated circuits, transistors, diodes, resistors, capacitors, and light emitting diodes (LEDs). Light-emitting diodes mounted on printed circuit boards provide status information regarding operation of the UPS units. Seven such LEDs are shown mounted horizontally. The alarm indicator board contains an additional 17 LEDs mounted vertically. Of these 24 LEDs, 11 provide indications for 10 parameters which isolate (turn off) the inverter in the UPS unit. The 10 parameters represented by the LEDs are alternating current (ac) undervoltage (shown as ACUV Slow and ACUV Fast), ac overvoltage, direct current (dc) undervoltage, dc overvoltage, UPS unit clock condition (shown as Clock Failed), UPS unit output frequency (shown as Freq. Failed), UPS unit control logic circuitry status (shown as Logic Failed), UPS unit control logic power supply condition (shown as PWR Supply

Failed), inverter leg fuse status (shown as Leg Fuse), and UPS unit normal power output source overload (shown as Overload Transfer). If any one of these parameters is not within pre-determined limits, then the corresponding LED should light indicating that the UPS inverter is isolated. The rapid isolation of the UPS inverter is required when any of these parameters are outside of their pre-determined limits in order to preclude improper operation, severe damage, and/or destruction of internal component parts.

Each of the remaining 13 LEDs provides status information for the operating UPS unit and, by design, is lit only if the corresponding parameter is outside of its pre-determined limits. None of the parameters associated with these 13 LEDs results in isolating the UPS inverter. In addition, the design of the UPS unit includes features for LED lamp testing and circuitry resetting. This feature is implemented by mechanical switches on printed circuit boards. These switches are shown in Figure 4.17 as Lamp Test/Unstore, Lamp Test - This Card Only, and Reset - This Card Only.

The display panel for the unit may be viewed with the UPS cabinet doors closed (Figure 4.18). This panel contains meters which provide information regarding electrical power inputs to and outputs from the unit. On the left side of the panel, ac voltage and amperage meters provide information regarding the normal ac input power to the unit. On the right side of the panel, ac voltage, current (amperage), and frequency meters provide information regarding the power output of the unit. The panel also contains various status lights to indicate circuit breaker positions. One two-position toggle switch is provided for opening and closing CB-3. A three-position toggle switch is included for power output transfer control permitting automatic and manual restart of the unit. Indicating alarms are provided for the inverter and charger (ac-to-dc converter) as well as for the UPS unit external dc battery supply. A module trip alarm indicator lights when the UPS normal power output source has been isolated.

UPS Control Logic Power Supply

The control logic power supply provides the required power to the unit's control logic. Should this power supply degrade below prescribed values, the unit is designed to open CB-1, CB-2, and CB-3, thus isolating the UPS inverter. If the maintenance supply meets the criteria enumerated above, electrical signals are provided to operate the static switch and close CB-4, thus providing power to the critical loads from the maintenance supply.

Figure 4.19 shows a simplified diagram of the control logic power supply for a 75-kVA 1-series UPS unit. (The 120-V ac maintenance supply is provided by the power regulator output). With switch S1 closed, the K5 relay is energized and phase B of the maintenance power supply is applied to the inputs of the control logic power supplies. These solid-state power supplies are designed to provide a regulated voltage output of plus and minus 20 V dc. They also act as a charger for the control logic power supply batteries when circuit elements S1 and S2 are closed. The solid-state power supplies and the parallel battery circuits form the power supply for the control logic required to operate the UPS 1-Series unit. There are a total of six battery packs per UPS unit, with each pack consisting of three individual cells. Each individual lead-acid cell is identical in size and shape to a D-sized flashlight cell and is rated for 2.5 ampere-hours, with a 10-hour discharge rate. The

specified operating temperature range for each cell is -20° Celsius (C) to +60° C. Float charge voltage for each cell is 2.3 V dc at 35° C. Each cell has a specified shelf life of 3 years at 25° C (77° F).

4.3.3 Post-Event Testing for the 75 kVA 1-Series UPS

Licensee personnel tested the UPS units with the UPS vendor (Exide Electronics) representatives and team members observing and advising. Key parameters were monitored using several digital volt meters and a dual trace digital storage oscilloscope. Most testing was done on UPS 1C and 1D since UPS 1A, 1B, and 1G were providing power to more important operating electrical loads.

Testing and troubleshooting demonstrated the following:

- (1) The dc control logic power supply for the five UPS units is normally provided power from the B phase of the maintenance supply. The inverter output power serves as a backup supply.
- (2) The trip point of the dc control logic is 17.3 V dc for UPS 1D, corresponding to 84.5-V ac input voltage to its power supplies; and 16.9 V dc for UPS 1C corresponding to 84.9 V ac. This trip results in the control logic providing an automatic signal to isolate the normal power output source for the unit. The control logic power supply dc output voltage decreases sharply as the ac input voltage decreases below approximately 92 V ac.
- (3) The transfer to alternate power is accomplished by way of the K5 relay. The K5 relay drop out voltage is 45 V ac for UPS 1C and the pick up voltage is 52 V ac. The K5 relay drop out voltage is 42 V ac for UPS 1D and pick up voltage is 55 V ac.
- (4) Voltage transients induced during troubleshooting on the normal 600-V ac 3-phase input power to UPS 1C did not trip the unit.
- (5) There are 18 control logic power supply batteries per UPS unit. The internal control logic power supply batteries on all five UPS units were not capable of providing adequate control logic voltage when all other sources were disconnected (see Tables 4.3, 4.4, and 4.5). With the current UPS design, there is no way to determine that the batteries are in a degraded condition during normal operation. The control battery discharge light (shown in Figure 4.19) represents the dc output voltage for each of the two power supplies and, by design, provides indication when either one of the dc output voltages decreases below a pre-determined value. The PWR (power) supply failed light indicates when the voltage applied to the control logic is below an acceptable level.
- (6) Voltage transients injected by dropping ac input voltage to near zero for 100-to-200 milliseconds on the maintenance power line, in combination with the

degraded batteries, trips the units without allowing the K5 relay to change state, a condition demonstrated on UPS 1C and UPS 1D units.

- (7) A sudden complete loss of the maintenance supply voltage with both new and degraded batteries installed did not cause an UPS unit trip. In this case, the ac input power for the control logic power supply properly transferred to the inverter output, thereby preventing an UPS unit trip.
- (8) Voltage transients induced on the maintenance power line, similar to these for item (6) above, with good batteries installed did not produce any UPS unit trips. However, some very short voltage perturbations on the control logic power supply were observed on the oscilloscope while testing UPS 1C and 1D units.
- (9) Fully charged battery cells are required for the successful transfer of relay K5 for severe degraded voltage conditions on the maintenance line since otherwise the UPS unit trips on control logic power supply failure (< 16.9 V dc with 84.5 V ac input) before the K5 relay will transfer the ac input power for the control logic power supply to the inverter output.

Table 4.3 Individual no-load battery pack recorded voltage for UPS 1C

<u>Old Battery Pack Voltages</u>	<u>New Battery Pack Voltages</u>
(1) 1.19 V dc	6.10 V dc
(2) 2.48 V dc	6.07 V dc
(3) 2.24 V dc	6.10 V dc
(4) 0.17 V dc	6.09 V dc
(5) 0.79 V dc	6.10 V dc
(6) 1.78 V dc	6.12 V dc

Internal no-load recorded voltage for the three positive and the three negative battery packs.

Positive: +0.6 V dc

Negative: +0.04 V dc (Note positive value here)

Table 4.4 Individual no-load battery pack recorded voltage for UPS 1D

<u>Old Battery Pack Voltages</u>		<u>New Battery Pack Voltages</u>
(1)	.254 V dc	6.1 V dc
(2)	.570 V dc	6.06 V dc
(3)	1.03 V dc	6.10 V dc
(4)	.07 V dc	6.10 V dc
(5)	1.17 V dc	6.13 V dc
(6)	1.39 V dc	6.09 V dc

Internal no-load recorded voltage for the three positive and three negative battery packs.

Positive: +0.6 V dc

Negative: +0.14 V dc (Note positive value here)

Table 4.5 Internal no-load recorded voltage for the three positive and three negative battery packs

<u>UPS 1A</u>	<u>UPS 1B</u>	<u>UPS 1G</u>
Positive: +0.7 V dc	Positive: +0.54 V dc	*Positive: +18.3 V dc
Negative: +1.1 V dc	Negative: +6.2 V dc	Negative: +0.69 V dc

*Correct no-load battery voltage is a necessary but not sufficient condition for a functional battery.

4.3.4 Principal Contributing Factors for Simultaneous Loss of Power Output from the 75 kVA 1-Series UPS

When the electrical fault occurred in the B phase main stepup output power transformer, in-plant B phase electrical distribution bus voltages were reduced by approximately 50 percent (see Section 4.2). This voltage reduction lasted about 200 ms. When the voltage reduction occurred, the comparator circuitry within the 75-kVA 1-Series UPS units detected this out-of-tolerance condition for the maintenance supply and precluded transfers to these sources by locking out electrical signals to operate each UPS unit CB-4 and parallel static switch. (see Figure 4.16.) This was a proper response for the 1-Series units. At the same time, the B phase maintenance supply continued to provide the ac power input to the control logic power supply since the degraded voltage values applied to the K5 relays were above the drop out voltages for these relays. (See Figure 4.19.) Because of this degraded ac input voltage and the severely degraded batteries, the dc output voltage of the control logic power supply decreased to below the logic trip setpoints for the UPS units and isolated the normal power output sources for each of the five units. Isolation of these sources, along with a transfer lockout, resulted in the loss of power outputs from the five UPS units.

The simultaneous loss of power outputs from the five 1-Series UPS units would not have occurred if the degraded voltage condition had not existed, or if the ac input power to the control logic power supplies was provided by the inverter power outputs, or if functional control logic power supply batteries had been installed in the units.

4.3.5 Pre-Event Documentation and Maintenance Activities for the 75 kVA 1-Series UPS Units

The licensee's electrical circuit drawings and equipment manuals for the five UPS units were not accurate, complete, or in agreement with each other and did not consistently reflect the actual installed units at the time of the event. Furthermore, the level of detail and completeness of the manual did not effectively communicate subsystem and major component function. The equipment manual did not clearly state the function and importance of the control logic power supply batteries. The electrical circuit drawings had to be furnished to the team by the manufacturer and were inconsistent. Because the manual was inadequate, the team was occasionally forced to trace electrical signals through complex schematic drawings to determine how the UPS units actually functioned.

This important information was also not apparent from the electrical circuit drawings. For example, more adequate documentation may have enabled the licensee to discover the control logic power supply preferred ac input source design deficiency and perform corrective actions which would have prevented this event. The labeling on the front panel of the UPS unit and in the equipment manual did not always reflect the actual function of a specific component. For example, the control battery discharge alarm indicator light does not represent the state of the control logic power supply batteries when the power supply is functional. If the control logic power supply is functional, the battery discharge alarm indicator light will be off, independent of the battery's condition. This could falsely suggest that the batteries are fully charged when, in fact, they may be completely discharged. The documentation is also confusing because it is for a generic UPS unit. The vendor designed

many optional features into the unit which were not utilized by the licensee. Unused optional features should have been documented as "not used" to avoid confusion.

The licensee's equipment manual stated that the inverter output was the preferred (primary) input power source for the control logic power supplies. This statement in the manual was inconsistent with the electrical circuit drawings. The units as actually installed employed the maintenance supply as the preferred input power source in accordance with the electrical circuit drawing. After the event, the equipment hardware was modified to coincide with the equipment manual statement instead of the vendor drawing. The equipment manual also stated that the replacement interval for the control logic power supply batteries was 4 years. The correct interval was subsequently determined by the supplier to be 1 year. Another error involving an alarm indicator light label was discovered. The front panel of the UPS unit reads "ac overvoltage" for the alarm indicator light located on the alarm printed circuit board (oriented vertically in Figure 4.17), and the equipment manual defines the same light as a "ac undervoltage" alarm.

A review of maintenance work order records for the 75 kVA 1-Series UPS units indicated that the maintenance consisted primarily of replacing air filters, recording meter and alarm indications, removing dust and dirt, and applying heat sink grease to SCRs. The records also showed no scheduled maintenance for the control logic power supply battery packs. If these battery packs had been fully functional during the transient, the UPS units would have maintained their power outputs. Therefore, improved preventative maintenance for the UPS, which included battery pack replacement, would have precluded this event. Subsequent to the event, the maintenance program was revised to include an appropriate replacement schedule for the control logic power supply battery packs based on supplier recommendations and actual service conditions.

The licensee did not have an in-place vendor support program which would have facilitated the exchange of UPS unit critical information. This information may have improved the documentation (equipment manual and electrical circuit drawings) maintained by the licensee and led to adequate maintenance practices by providing the licensee with an opportunity to consider acquiring design enhancements and to question the installed configuration.

4.3.6 Post-Event Corrective Actions for the 75-kVA 1-Series UPS

Post-event corrective actions for the five 1-Series UPS units involved modifications to wiring, replacement of the six battery packs in each of the five UPS units, revisions to selected UPS unit normal feeder breaker settings, and replacement of specific circuit breakers on selected UPS units.

The UPS internal wiring was modified such that the K5 relay (Figure 4.19) is normally energized from the inverter output rather than the maintenance supply. Contacts associated with the K5 relay were also rewired such that with this relay energized the ac input power to the control logic power supply is provided by inverter output power. With this arrangement, the inverter output power is the preferred source of input power to the control

logic power supply, the maintenance supply as the alternate. Battery packs in the five UPS units were replaced with fully charged batteries.

A few circuit breaker problems were experienced during the August 13, 1991 event and during subsequent troubleshooting activities. The feeder breaker to UPS 1A tripped twice while the damage control team was attempting to restore the normal power output source for the unit. In February 1991, the overcurrent adjustable trip setting on the ac feeder breaker was adjusted to the lowest setting as part of a program to define trip settings on each plant breaker with an adjustable trip setpoint. The adjustment was done in accordance with standard practice of estimating inrush current based on six times the normal UPS load of 90 amperes. The 1-Series UPS vendor has subsequently advised the licensee that inrush current can actually be six to ten times normal load. Consequently, the overcurrent trip setpoint has been revised. The same changes have been made to the feeder breakers for UPS 1B and 1G. This situation is not applicable to UPS 1C and 1D because of a different breaker coordination scheme for these units. Another breaker problem occurred on UPS 1B when CB-3 would not close. This problem had been identified prior to the August 13, 1991, event and the breaker was to be replaced. A new replacement breaker was installed as a corrective maintenance action on UPS 1B and 1D. The final problem involved CB-2 on UPS 1D. The licensee has documented that this breaker had a greater number of operational cycles in its lifetime than the CB-2 breakers on the other 1-Series UPS units. In addition, the licensee documented that during troubleshooting activities, CB-2 on UPS 1D was cycled an additional 15 times and finally would not close. It has been replaced with a new one as a corrective maintenance action.

4.3.7 Description of Safety-Related 2-Series UPSs

Figure 4.20 shows a simplified diagram for the safety-related 2-Series UPS. Normal 600-V ac 3-phase input power is provided to the unit from safety-related electrical distribution buses. The maintenance supply (alternate) 600-V ac single phase input to the unit is provided by a different safety-related electrical distribution bus. The principal internal elements of the 2-Series UPS unit are an input circuit breaker (CB-51), an ac-to-dc converter, a battery disconnect circuit breaker (CB-52), a blocking diode, a dc-to-ac inverter, a static switch, and an output circuit breaker (CB-53). With the exception of the static switch, the other elements are functionally identical to comparable elements provided for the 75-kVA 1-Series unit and are as described in Section 4.3.2 of this report. The static switch internal to the 2-Series UPS is a fully rated solid-state device and, as such, is designed to provide continuous rated power output from the unit to the safety-related electrical loads by way of the vital bus. Electrical protection for the static switch is provided by fuses should electrical faults develop.

Elements external to the 2-Series unit include a maintenance supply input circuit breaker (CB-1), a transformer regulator unit, a static switch input circuit breaker (CB-2), and a two-position maintenance bypass switch (S1). Electrical protection for the transformer regulator unit is provided by fuses and an upstream circuit breaker. The transformer regulator unit provides a two percent regulated output for a range of input voltage values. The two-position make-before-break maintenance bypass switch is provided to permit maintenance on the unit.

UPS Control Logic

The control logic for the 2-Series unit provides automatic electrical signals to the ac-to-dc converter, dc-to-ac inverter, CB-51, CB-52, and the static switch. These signals are required for proper operation of the unit. Control logic comparator circuitry permits the static switch to transfer the unit's power output from the inverter to the maintenance supply if the differences in voltage amplitude, frequency, and phase angle between the inverter output and the maintenance supply are within established limits. These limits are 10 percent, 0.5 Hz, and 5° for voltage amplitude, frequency, and phase angle, respectively. The control logic also provides automatic signals to CB-51, CB-52, and the static switch to isolate the normal power output of the unit when required.

UPS Control Logic Power Supply

Figure 4.21 shows a simplified block diagram for the 2-Series UPS unit. (The alternate 120-V ac maintenance input supply to the unit is not shown.) The power supply for the unit's control logic is obtained from a dc-to-dc converter. The input power to this converter is obtained from a safety-related Class 1E battery bus. With this arrangement, the dc power for the control logic is less susceptible to voltage perturbations in the in-plant electrical distribution system than the arrangement for the 75 kVA 1-series UPS units.

4.3.8 Other Potential Causes and Anomalies Investigated

The team investigated other potential causes and anomalies relevant to the simultaneous loss of power outputs from the five UPSs. These items were propagation of high frequency noise from the main transformer fault, a voltage transient on the station ground system, and the reported alarm indication anomalies for the five UPSs.

The transmission of high frequency noise from the transformer fault both through the atmosphere and through the station's electrical distribution system to the UPS was evaluated as a cause for the loss of power outputs from the units. Initial in-plant acceptance tests were performed for the 75-kVA 1-Series UPS units in May 1985. One of these tests involved keying a hand-held radio frequency (RF) transmitter positioned about 2 feet from the UPS cabinet sides and front doors. This test was performed with the cabinet access doors open and closed. The test results demonstrate that these units are not sensitive to RF transmissions through the atmosphere unless the cabinet access doors are open and the RF source is near electrical circuitry internal to the unit. In addition, because of intervening transformers in the electrical distribution circuit that filter such signals, the possibility that high frequency noise could have been transmitted through the station ac distribution system to the UPS units is considered to be remote. For these reasons, this potential cause is not considered credible.

A voltage transient on the station ground system is considered unlikely because one of the five UPS units which lost power output is physically located far from the other four units, yet it exhibited similar behavior. No other station equipment, including other UPS units, had the functional damage that usually accompanies voltage transients on the station grounding system. In addition, laboratory tests show that a significant ground transient

would have caused the destruction of numerous electrical and solid-state circuitry components. This was not the case at NMP-2. Thus, a significant voltage transient on the plant grounding system as a probable cause for the simultaneous loss of power outputs from the UPS units is considered extremely remote.

Operations personnel who restored power outputs to the five UPS units reported on initial conditions and alarm indications. Each stated that the data provided was accurate based on their recollection, but that it was possible they did not remember everything. For instance, operations personnel could not state positively whether or not they reset the alarm indications on the UPS 1D unit. The conditions common to the five UPS units were: CB-1 tripped (open), CB-2 tripped (open), CB-3 open, CB-4 open, the two position toggle switch CB-3 (shown in Figure 4.18) in the closed position, and the three-position toggle switch in the auto restart position (Figure 4.18). In addition, all units except UPS 1D had the module trip alarm light on. All units except UPS 1D and UPS 1G had the inverter logic alarm light on. Only UPS 1D and UPS 1G had the voltage difference and output overvoltage/undervoltage (OV/UV) alarm lights on. Only UPS 1D had an UV/OV transfer alarm light on. Everyone present thought, but were not absolutely positive, that none of the 10 LEDs (upper right hand corner of Figure 4.17) that indicate the initiating signals for a module trip were lit. Lastly, each operator stated that absolutely no alarm indication had been reset on UPS 1G.

The reported data clearly suggests that there were UPS alarm indicator light anomalies in this event. They can be divided into three categories. The first pertains to the deviation in alarm indications between the individual UPS units. Each of the five UPS units lost its power output due to a common cause; therefore, it would then be expected that the alarms generated by the individual UPS units would be identical. Operations personnel attempting to restart UPS 1D likely reset the alarm indications, which may explain this unit's module trip and inverter logic alarm indicating lights being off. Although there are internal adjustable alarm indicator setpoint variations between the individual UPS units, this cannot adequately explain the deviations in the reported alarm indications.

The second category of light anomalies involves reports that on certain UPS units the module trip light was on while none of the 10 latched LEDs alarm-indicating lights were on. Any one specific parameter associated with these 10 LEDs, if out of tolerance, will initiate an UPS module trip and turn the module trip light on. After reviewing the electrical circuit drawings, the team found that there are direct "latch-free" circuit paths through various logic circuit elements from the parameter alarm light driver circuit elements to the module trip light. Since there were no other trip signals, at least 1 of the 10 LEDs alarm indicating lights must be latched on to hold the module trip light on. The cause of this anomaly is not known.

The third category of reported light anomalies originates from the reported off-state of the voltage difference and OV/UV lights on certain units. Of all the nonlatched alarm indicating lights, at least these two should have been on continuously until the closure of CB-4. When operations personnel initially arrived at the UPS units, there was a voltage difference between critical buses and the bypass source inputs because the bypass source was available and CB-4 was open. For a similar reason, there was an undervoltage condition

on the UPS units' critical buses. There is no adequate explanation at present as to why the logic circuitry did not sense and indicate these conditions.

There are two possible general explanations for the reported light anomalies. First, the data reported by the operations personnel may be erroneous. Inaccuracies could occur because of unreported UPS restoration activities (i.e., resetting the alarm indications) performed by the operations personnel before they inspected the alarm-indicating light status or simply because they incorrectly recalled what they saw in a stressful situation.

The second possible explanation for the reported light anomalies is that a circuit malfunctioned. There has been considerable effort devoted to this issue, mostly by Failure Prevention, Inc. They conducted tests on one of the installed UPS units in the laboratory using a test fixture setup of several alarm printed circuit boards that were in use during the event. The goal of the testing was to conclusively explain the alarm indicator light anomalies. Circuit malfunctions were easily induced by subjecting the circuitry to one or a combination of control logic power supply voltage transients, ground voltage transients, increased temperatures, light exposure, and electromagnetic interferences. (Note that there are no data to indicate that any of these conditions did or did not exist during the actual event.) Nevertheless, the alarm light anomaly involving the module trip indicating light was reproduced numerous times in the laboratory. However, the simulated conditions for these reproductions are considered unlikely to have been generated during the event. They do, nevertheless, demonstrate that the alarm board is capable of exhibiting the anomaly. Thus, a circuit malfunction may not be accepted or rejected as either the cause or as a contributing factor for the light anomalies.

4.4 Major Uninterruptible Power Supply Loads

The five uninterruptible power supplies (UPSs) that lost output power during this event provide power to important balance-of-plant (BOP) equipment. These loads are listed in Tables 4.6, 4.7, and 4.8 at the end of Section 4.4. UPS 1A and 1B power the instrumentation and controls that operators frequently use for normal operations, while UPS 1C and 1D power the essential lighting and plant communications equipment. UPS 1G powers the plant process computer and the digital radiation monitoring computer. For some equipment, UPS 1A and 1B act as backup for each other. In addition, the turbine functions on UPS 1A have a motor generator backup. Loss of UPS 1C or 1D will result in only a partial loss of lighting and communications.

Failure to power the critical loads normally supplied by UPS 1A will inhibit control rod movement (except for a reactor scram); partial fail as-is RCS recirculation flow control; cause loss of rod position indication; cause partial loss of control room annunciators and partial loss of the paging system; lose LWS and SPDS computers; cause partial loss of drywell cooling; and loss of several BOP monitoring systems.

Failure to power the critical loads normally supplied by UPS 1B will inhibit control rod movement (except for a reactor scram); partial fail as-is the RCS recirculation flow control; cause failure as-is for feedwater flow control valves; cause partial loss of drywell cooling; loss of fire protection panel and partial control room annunciators; cause partial losses of

plant paging and walkie talkies, and cause full loss of BOP recorders and area radiation monitoring.

Failure of both UPS 1A and 1B fail open the mini-flow valves to feedwater, condensate booster, and condensate systems; fail the neutron flux recorders; and fail fourth-point heater drain pump controls. These will result in a trip of feedwater pumps and a possible reactor scram.

Failure to power the critical loads normally supplied by UPS 1C will cause partial losses of essential lighting, egress lighting, paging, and stack GEMS. Failure to power the critical loads normally supplied by UPS 1D will cause a partial loss of essential lighting, egress lighting, paging, and the dial telephone. Failure to power the critical loads normally supplied by UPS 1G will cause loss of the plant process computer, the digital radiation monitoring computer, the meteorological monitor, the fire panel computer, and the 3-D monicore computer.

In response to I&E Bulletin 79-27, the licensee prepared a failure mode and effects analysis (FMEA). This analysis was a very detailed review of instrumentation on each bus, including the Class 1E and non-Class 1E UPS, to determine the impact of their loss on plant and instrumentation required to bring the reactor to a safe shutdown. The team notes that all the components affected on August 13, 1991, are listed in the analysis. The licensee appeared to have produced the load list that the team requested while on-site from scratch without knowledge of the existence of the FMEA. Because of this the team was able to validate that both the information from the FMEA and licensee agreed as to the power sources to the components affected in this event. The FMEA was important to the team in providing insights of the impact of losing each UPS.

Important components that could scram the plant, such as the condensate and feedwater system recirculation mini-flow control valves and fourth-point heater drain pump controls are powered by UPS 1A and UPS 1B. The important functions, such as steam bypass regulation, have UPS 1A main power and a small motor generator as a backup. This means that should UPS 1A be lost, the plant would not necessarily scram. In fact, UPS 1A was lost last February 1990 for a short time and the plant did not scram. (See Section 6.2.1 for a discussion of the February 1990 event.) The control room annunciator panels have one preferred source, either UPS 1A or 1B. If the preferred source is lost, then the alternate source of UPS 1A or 1B takes the added loads. Unfortunately, for NMP-2, the worst load determined by the number of annunciators lit might trip the alternate circuit when the load is transferred. Should this occur, the annunciator's circuit would be lost, although other instrumentation and control would continue to be powered. This licensee is investigating this potential circuit failure.

Electronics cabinets for instrumentation and control of the feedwater and condensate system contain internal redundant power supplies which provide dc power to the electronics. One power supply is connected to UPS 1A and the other to UPS 1B. If one internal power supply fails, the other internal power supply will continue to power the electronics. If one UPS fails, the other will continue to power the associated internal power supply. Hence, there is internal redundancy within the system.

Random failures of individual components or subsystems would not have caused the August 13 incident. But, even though the systems are redundant, they are not diverse and, as a result, were vulnerable to the common-mode failure of multiple UPSs described in Section 4.3. This power redundancy does not apply to all the components. For instance, the rod position indication system (RPIS) takes power from only UPS 1A, so that the failure of UPS 1A alone would cause loss of control rod position indication. However, such a loss would not cause loss of the feedwater condensate or turbine systems, for which automatic scram or manual-controlled shutdown would be required.

Table 4.6 Major loads on uninterruptible power supply 1A

1.	Control Rod Reed Switches
2.	Rod Position Indication System (RPIS)
3.	Rod Sequence Control System (RSCS) — UPS 1B Backup
4.	Rod Worth Minimizer (RWM)
5.	Digital Memory Module (DMM) — UPS 1B Backup
6.	Four Rod Display
7.	Rod Withdrawal Inhibit
8.	Gaseous Effluent Monitoring System (GEMS)
9.	Vent GEMS
10.	Liquid Rad Waste System (LWS) Computer
11.	LWS Control
12.	Safety Parameter Display System (SPDS)
13.	Emergency Response Facility Functions
14.	Emergency Operating Facility Computer Link
15.	Controllers to Condensate Booster, Condensate and Feedwater Mini-Flow Valves - UPS 1B Backup
16.	Fourth-Point Heater Drain Pump Controls — UPS 1B Backup
17.	Partial Control Room Annunciators — See Note
18.	Cooling Water Bypass Gates (MOV 52s)
19.	Partial Paging System (Gaitronics)
20.	Partial Reactor Recirculation Control
21.	Post-Accident Sampling System (PASS — A Train)
22.	Partial Drywell Cooling
23.	Steam Bypass Control — Motor Generator Backup
24.	Turbine E/H and Trip Functions — Motor Generator Backup
25.	SRM Recorder — UPS 1B Backup

Table 4.6 Major loads on uninterruptible power supply 1A (cont.)

-
26.	IRM/APRM, IRM/APRM/RBM Recorder — UPS 1B Backup
27.	Recirculation Flow Recorder — UPS 1B Backup
28.	Safety-Relief Valve Temperature Recorder
29.	Cooling Water Monitoring
30.	Jet Pumps Monitoring
31.	CRD Monitoring
32.	Turbine Monitoring
33.	Condenser Monitoring
-

Note: This table does not include all the circuits associated with BOP instruments. Control room annunciator circuits will switch to UPS 1B when UPS 1A fails.

Table 4.7 Major loads on uninterruptible power supply 1B

-
1.	Digital Memory Module (DMM) — UPS 1A Backup
2.	Rod Sequence Control System (RSCS) — UPS 1A Backup
3.	Rod Withdrawal Inhibit
4.	Feedwater Control System (FWCS)
5.	Controllers to Condensate Booster, Condensate and Feedwater Mini-Flow Valves — UPS 1A Backup
6.	Partial Reactor Recirculation Control
7.	Fourth-Point Heater Drain Pump Controls — UPS 1A Backup
8.	GE Transient Analysis Recorder System (GETARS)
9.	Partial Control Room Annunciators — See Note
10.	Partial Walkie Talkies (Leaky Wire Radio System)
11.	Partial Paging (Gaitronics)
12.	Control Room Fire Protection Panel
13.	Partial Drywell Cooling
14.	Post Accident Sampling Station (PASS-B Train)
15.	SRM Recorder — UPS 1A Backup
16.	IRM/APRM, IRM/APRM/RBM Recorders — UPS 1A Backup
-

Table 4.7 Major loads on uninterruptible power supply 1B (cont.)

-
17.	Off Gas Radiation Monitor
18.	Recirculation Flow Recorder — UPS 1A Backup
19.	Radiation Area Monitoring
20.	Radwaste Radiation Monitoring
21.	Radon Area Monitoring
22.	Turbine Monitoring
23.	Generator Monitoring
24.	RCS Monitoring
25.	RPV Normal Monitoring
26.	RHR Monitoring
27.	RWCU Monitoring
-

Note: This table does not include all the circuits associated with the BOP instruments.
Control room annunciator circuits will switch to UPS 1A when UPS 1B fails.

Table 4.8 Major loads on uninterruptible power supply 1C, 1D, and 1G

<u>UPS 1C</u>	<u>UPS 1D</u>	<u>UPS 1G</u>
1. Partial Essential Lighting	1. Partial Essential Lighting	1. Plant Process Computer
2. Partial Egress Lighting	2. Partial Egress Lighting	2. Digital Radiation Monitoring Computer (DRMS)
3. Partial Paging	3. Partial Paging	3. Meteorological Monitor
4. Stack GEMS	4. Dial Telephone	4. Fire Panel Computer
		5. 3-D Monicore Computer

Note: This table does not include all the circuits associated with the BOP instruments.

4.5 Instrumentation and Controls

Sections 4.5.1, 4.5.2 and 4.5.3 discuss the safety-related and balance of plant (BOP) instrumentation important to the event of August 13, 1991. BOP instrumentation for neutron flux and control rod position indications is discussed in Section 4.5.1. Section 4.5.2 discusses losses of other BOP instrumentation that is routinely used by operators and explains why systems failed the way they did. The safety-related instrumentation that did not fail, that was instrumental in providing indications during the event, and that provided the only record of the event, is discussed in Section 4.5.3.

4.5.1 Control Rod Position Indication and Neutron Monitoring

During the August 13, 1991, event both control rod position and neutron monitoring became critical parameters because operators needed both indications to confirm that the reactor was shutdown. In addition, the operators went into an anticipated transient without scram (ATWS) procedure when the position of control rods could not be determined. For a fuller description of these procedures and operator actions, see Section 5.3.

The reactor manual control system contains the subsystems which provide control room operators their indication of control rod position. This system includes the rod position indication system (RPIS), rod drive control system (RDCS), rod sequence control system (RSCS), rod worth minimizer (RWM), and the digital memory module (DMM), normally referred to as the full core display. In addition to these subsystems, the operator can display multiple rod positions using the four rod position display. The plant process computer (PMS) monitors control rod positions and sends information to the alarm printer. Figure 4.22 shows a diagram of the system.

Within the control rod structure are a string of reed switches that run the length of the rod. They signal the rod's physical position. In the RPIS, the information from the control rod is converted to status data and sent to the other subsystems.

For example, when the RWM receives the rod position signal, "00," it interprets it as indicating that the control rod is full-in. Once the control rod is full-in or at "00," a "latch" function in the software holds the rod's full-in signal. The RSCS receives the rod position signal from RPIS and validates the quality of data. The DMM receives the rod position full-in signal from RSCS, using it to light the full-in light on the control room full core display (Figure 4.23).

The RDCS is designed to stop (i.e., lockup) control rod movement when power is restored to prevent erroneous control data from being sent to the rod directional control valves. The four-rod display allows the operator to specify a rod's location to determine information about the three adjacent rods. When operators select rods using the RSCS, those selected are identified on the full core display.

After restoring power to the UPS, and before restarting the RDCS, and resetting the scram signal, the operators were receiving conflicting information from the control rod indicators. RSCS indicated that 15 rods were not full in. DMM indicated that six rods were not full in. RWM indicated that all rods were full in. The four-rod display indicated blanks when each of these six rods were selected. RDCS was "locked up" (i.e., could not move). The reason for the discrepancy

in rod position results from differences in the design of the subsystems in determining when all the rods are full in. All of the subsystems look at the position signal for the full-in data; then RSCS and RWM look for different additional information to conclude that the rods are in. Three burned out lights bulbs found in the DMM account for three of the six false signals for control rod position.

The team determined that the control rod reed switches, RSCS, DMM, RWM, and four rod display were all powered from UPS 1A. The RSCS and DMM do have alternate power from UPS 1B but the reed switches and RPIS, which process the data, are powered only from UPS 1A. Table 4.9 details characteristics pertinent to this event.

The neutron monitoring system is used to detect neutron flux in the reactor core over a wide range from shutdown conditions to full power operations. In addition to the wide range, the spatial distribution of the neutron flux is needed to assure that operating limits are not exceeded at any location within the reactor core. The neutron monitoring system consists of three types of overlapping range monitors: average power range monitors (APRM), which includes linear power range monitors (LPRM), intermediate range monitors (IRM), and source range monitors (SRM). Both the IRMs and SRMs are retractable detectors that are motor-driven into the core by the operators when required.

The SRM is used when the reactor is fully shut down and during startup. Source range is from 0.1 to 1×10^6 counts per second (cps). The IRM overlaps the source range and extends into the power range. Intermediate range is from 4×10^{-5} to 12.6 percent power. The LPRM overlaps the IRMs. Linear range monitors are functional from 0.5 to 125 percent power while APRMs are functional from 0 to 125 percent power. APRMs indicate average power calculated from the LPRMs fixed incore detectors. Rod block monitors (RBM) use the LPRM similar to APRM to prevent rod movement and operational nuclear power limits from being exceeded. Table 4.10 provides the important characteristics of these instruments.

APRM front panel 603 indication is only on a recorder as is the indication for IRM, except that IRM also has status lights. LPRM front panel 603 indication is on meters that display the selected rod information from the four-rod display. SRM front panel indicators are on a recorder and meters. All neutron monitors have indication status lights and meters on back panels 606, 608, and 633.

When the five one-series UPSs were lost, most of the front panel neutron indications were lost. This lost power affected only the recorders. The power to the monitors was still available. Even though the signals were good going into the recorder, the recorder contains an amplifier circuit that takes the signal and amplifies it to mechanically move the indicator pointer. These amplifier circuits are powered from the lost UPS. Therefore, the recorders failed as-is showing 100 percent indication for the APRM. The LPRM display was also inoperable due to the UPS loss. See Figure 4.24 for the physical location of the indicators.

Tables 4.9 and 4.10 list important characteristics of display, and power source for the control rod position indication and neutron flux monitors. Both the control rod position and the neutron flux monitors were utilized by operators during the event.

The APRM recorders that were lost are crucial front panel indicators to the operators and with most of the rest of panel 603 instrumentation inoperative, the team noted that the operators did not initially trust or believe any neutron flux indicators (see Figure 4.25). Therefore, the operators had to resort to going to the panels at the back of the control room (see Figure 4.26). It is noted that on loss of all normal power, the IRM and SRM, which need to be driven into the core, would be inoperable. In addition, the neutron flux indications cannot be relied upon in some accidents since the components are not fully qualified.

Control rod position indication has only one power source to the reed switches. Therefore, if UPS 1A fails, then all control rod position indicators are lost. Loss of UPS 1A creates further complications since most of the indicating systems, with the exception of the plant process computer, have this UPS in common. Unlike the neutron flux indication, control rod position has only front control room indications. The team notes that control rod position indication, just like the neutron flux monitor, cannot be relied upon in some accidents since most of the components are not fully qualified.

Table 4.9 Control rod indicators

Instrument	Power	Class IE	Indication Location	Status of Indication
Full Core Display (DMM)	UPS 1A UPS 1B	No	P603	Full core display panel went dark.
Rod Sequence Control System (RSCS)	UPS 1A UPS 1B	No	P603	Rod sequence control system panel went dark.
Rod Worth Minimizer (RWM)	UPS 1A	No	P603	Rod worth minimizer display went dark.
Four Rod Display	UPS 1A	No	P603	The four-rod window display went dark.
Rod Position Indication System (RPIS)	UPS 1A	No	Not Applicable	There is no direct indication. The indication is through the subsystems that use the information.
Plant Process Computer (PMS)	UPS 1G	No	Located within the control room	The plant process computer CRT went dark.

Class 1E - Criteria are provided in IEEE Standard 308-1980

Table 4.10 Neutron flux monitor indicators

Instrument	Power	Class 1E	Indication Location	Status of Indication
APRM	UPS3A UPS3B	No	P603 B608	Inoperable due to loss of recorder Down scale status lights, meter on back panel operable
LPRM	UPS3A UPS3B	No	P603 B608,633	Inoperable due to loss of 4-rod display Down scale status lights, meter on back panel operable
IRM	24vdc	No	P603 B606,633	Inoperable recorder indication, status lights operable Back panel status lights and meter operable
SRM	24vdc	No	P603 B606,633	Inoperable recorder indication, meter operable Back panel status lights and meter operable
APRM/IR/SRM Recorders	UPS1A UPS1B	No	P603	Recorders inoperable frozen at full power All indications on these recorders inoperable
IRM Drive	120vac	No	Not Applicable	Driven into the core +2 minutes, power is from normal ac
SRM Drive	120vac	No	Not Applicable	Driven into the core +15 minutes, power is from normal ac

Class 1E-Criteria are provided in IEEE Standard 308-1980.

P = Front Panel

B = Back Panel

4.5.2 Other Balance Of Plant Instrumentation

During the August 13, 1991, event, a multitude of balance of plant (BOP) instruments failed. BOP instrumentation is important in normal plant operations and is used routinely by operators. This instrumentation is considered important equipment and is, therefore, powered by reliable sources, which in this case, are the nonsafety-related UPSs. The mode of failure is important in order to provide more information about the event. All of this failed equipment, with the exception of the safety-related hydrogen oxygen sample pump, is commercial grade.

Control Room Annunciators

The control room annunciators are powered from both UPS 1A and UPS 1B. The few annunciators that were reported functioning after loss of the UPSs have backup batteries. If one of the UPS is lost, the other UPS will take up the extra load. Depending on the number of annunciators on at the time of the transfer, it is possible that all annunciation would be lost because of an overload on the supply circuit.

Plant Computer Systems

Computer systems at NMP-2 include: (1) plant process computer/plant monitoring system (PMS), (2) liquid radwaste (LWS) computer, (3) digital radiation monitoring system (DRMS), (4) gaseous effluent monitoring system (GEMS), (5) GE transient analysis recorder system (GETARS), (6) 3-D Monicore, and (7) the meteorological computer. None of these is safety related and all receive power from the five UPSs that were lost (see Section 4.4). The PMS processes a broad range of plant information. The liquid radwaste system (LWS) computer controls the LWS, emergency response facilities (ERF) functions, and safety parameter display system (SPDS). The digital radiation monitoring system (DRMS) and gaseous effluent monitoring system (GEMS) provide the process and effluent radiological monitoring, sample systems, area radiation, and airborne radioactivity monitoring. The GEMS system includes a mini-computer in the turbine building and two skids sometimes called vent GEMS and stack GEMS. The vent and stack skids can stand alone without the minicomputer, but only provide local indications. GETARS records vital parameters for transient analysis. The 3-D Monicore computer is used for core calculations and core monitoring. The meteorological computer processes meteorological data for display in the site emergency response facilities (ERF).

Most of these computers acquire the same data either from a common sensor or from each other. When the UPSs were lost, all the computer systems went down, with the exception of the stack GEMS, which receives power from UPS 1H. When power was restored, the GEMS was not communicating properly with the other systems. The GEMS mini-computer and the PMS had to be restarted to restore them to their proper working order. The safety-related monitors that feed the radiation computers were never lost and were providing display information in the control room through dedicated indicators.

Drywell Cooling and Off-Gas Isolation

Drywell cooling was lost during the event because the unit cooler loss of coolant accident (LOCA) override and valve position logic circuits had no power from UPS 1A and UPS 1B. Off-gas isolation occurred because of the loss of radiation monitors RE-13A and B, which fail high on loss of UPS.

Group 9 Valve Isolation

Group 9 valves are safety-related primary containment structure isolation valves which are normally closed. They function to limit the release of radioactivity. Their isolation signals come from the standby gas treatment system (SGTS) radiation monitor, high drywell pressure, reactor low water level, and manual isolation of MSIV. The team concludes that the isolation occurred during the UPS restoration because SGTS radiation monitor RU-105 failed high. The false high radiation signal was not transmitted because the transmitters were also lost with the UPS, but the transmission was completed upon UPS restoration.

Cooling Tower Bypass Valves

Motor-operated gates valves (MOG-52A,B&C) opened. The temperature instruments powered from UPS 1B fail downscale, which is also an indication of cold temperature. The gates valves opened on sensing the false cold temperature signal.

Plant Communications

NMP-2 has five plant communication systems: (1) dial telephone system, (2) radio communication system, (3) paging system, (4) maintenance and calibration communication system, and (5) sound powered communication system. The dial telephones provide communications to selected office areas and selected locations inside and outside the plant. The dial telephones are connected to the NMP-2 telephone system for normal telephone service and receive power from UPS 1D. The portable radio (walkie talkie) is provided for communications within the plant. This system utilizes a "leaky wire" radio system which is fed from UPS 1B. The paging system is used for public address and channel communications (see Figure 4.27). The system is powered from UPS 1A, 1B, 1C, and 1D. The maintenance and calibration communication system, used when testing and calibrating activities are carried on, is powered from normal ac power. The sound-powered communication is also used mostly for testing and calibrating. This system does not require electrical power.

The most readily available normal communication systems at the failed UPSs were the walkie-talkie and paging systems. Neither of these systems was available during the event, so that communications at the UPS area were lost.

Fire Protection Panel

The main control room fire protection panel indicates the status of information from smoke and fire detectors located throughout the plant. During the event, the fire protection panel

powered from UPS 1B was not available. The local fire monitoring panels are powered from normal ac and have backup power. In addition, with the exception of two local fire monitoring panels, the other local fire monitoring panels have internal batteries. Shortly after the event, as a precautionary measure, a roving fire brigade was dispatched. With the exception of the loss of control room annunciation, the ability to control a fire was not lost.

Containment Hydrogen/Oxygen Sample Pump

During the event, sample pump P2B tripped, but pump P2A did not. Both pumps are safety related. Post-event trouble-shooting revealed that the panel was wired correctly but the cause of the tripping could not be determined.

Reactor Vessel Narrow Range Level

During the event, narrow range (NR) level A indicator went downscale while NR level B and C indicators stayed high. Since all three indicators are measuring the same level, the operators did not trust any of the readings. The power to the NR A indicator is from failed UPS 1A which accounts for the downscale reading. The other two indicators are from the normal ac power, which did not fail. These indications were in fact operable.

4.5.3 Safety-Related and Post-Accident Monitoring Instrumentation

Regulatory Guide (RG) 1.97, Revision 2, May 1988, provides guidelines for instrumentation to be utilized after an accident to assess plant status. NMP-2 licensee is committed to the guidelines in RG 1.97. RG 1.97 classifies plant variables for function (Types A, B, C, D, and E) and the applicable qualification criteria (Category 1, 2, and 3). Of prime importance are the variables classified as Type A or Category 1. Either of these two classifications requires that instrumentation be fully qualified to RG 1.97 criteria. Type A variables provide primary information to control room operators to act upon since they have no automatic actuation. While Type B through D variables are prescriptive, Type A variables are designated by licensee's since they are plant- and procedure-specific.

NMP-2 designated containment structure hydrogen and oxygen sample pumps, reactor pressure, reactor water level, suppression pool water temperature, drywell atmosphere temperature, and drywell atmosphere pressure as Type A variables. RG 1.97, Rev. 3, designates neutron flux monitors as a Category 1 variable but refers only to the APRMs and the SRMs. NMP-2 has not classified the neutron flux monitor as Type A, but has committed to install a Category 1 system when one is commercially available. (See Section 7.3 for a discussion of the BWR Owners' Group position on neutron flux. See Section 4.5.1 for a further description on the system and Table 4.10 for critical criteria of neutron flux.)

The other critical instrumentation in the event was the control rod position indication, which RG 1.97 classifies as Type B, Category 3. The licensee exceeds the RG 1.97 power supply criteria by providing power from UPS 1A. The rod position information is from the full core display (DMM)). (See Section 4.5.1 for further description of the system and Table 4.9 for critical criteria regarding control rod positions.)

All the RG 1.97 Type A variables are included as parameters in Technical Specification 4/3.3.7.5, "Accident Monitoring Instrumentation." The Accident Monitoring Technical Specification lists a total of 16 parameters that are safety related. Although one of two containment oxygen and hydrogen sample pumps tripped in the event, the rest of the safety-related instrumentation was operable.

The licensee classified reactor pressure and water level post-accident monitoring (PAM) instruments as Type A variables. Therefore, these systems are fully qualified and are powered from safety-related power. The PAM recorders are on control room panel 601 on a red background designated as "RG 1.97 variables" (see Figure 4.28). The reactor pressure and water level recorders provided the only chart recording of the sequence of events on August 13, 1991. All of the other sequences of events equipment failed with the loss of the UPSs.

4.6 Condensate and Feedwater Systems

The condensate and feedwater systems return water from the condenser to the reactor by a series of pumps, where the liquid is heated and made into steam. The steam is transported to the turbine by the main steam system. At the turbine, energy is extracted from the steam which is then converted to water in the condenser. This cycle is continuous in a normally operating BWR.

The condensate system consists of three condensate pumps (2CNM-P1A, P1B, and P1C) which supply water to three condensate booster pumps (2CNM-P2A, P2B, and P2C) which supply the feedwater system. The feedwater system (FWS) consists of three 50-percent capacity electric motor-driven feedwater pumps (2FWS-P1A, P1B, and P1C), along with high pressure and low pressure feedwater heating strings. The system is designed to deliver approximately 15 million lb/hr feedwater at 1055 psig and 420° F to the reactor vessel with two reactor feed pumps in operation. Each feed pump discharge line has its own 10-inch minimum flow recirculation line and a minimum flow-control valve for pump protection. This flow control valve is modulated to maintain a minimum flow through each pump. Each condensate booster pump also has its own minimum flow valve, while the condensate pumps are provided with a common minimum flow valve. All the minimum flow valves return flow to the main condenser (see Figure 4.29). The minimum flow valves (FWS-FV2s, CNM-FV38s, and CNM-FV114) are normally powered from UPS 1A (Foxboro Control) with UPS 1B as backup.

During normal reactor operation, the reactor water level is regulated by a feedwater controller which receives inputs from reactor water level and steam and feedwater mass flow rates (a three-element control). At low power levels, the controller receives input only from reactor water level (a single-element control). The feedwater control system adjusts the feedwater flow to maintain the desired reactor water level by generating signals which regulate the opening or closing of level control valves. The feedwater control system (FWCS) is powered by UPS 1B (Bailey Control).

Each feedwater pump discharge line has a feedwater level control valve (LV10A, B, and C). In addition, feedwater pumps A and B each have a high pressure/low flow control valve (LV55A and B), each designed to pass 7.5 percent rated nuclear boiler flow during reactor startup and low power operation. A low pressure/low flow control valve (LV-137) is provided for controlling flow while bypassing the feed pumps when the reactor is shutdown and at low temperature and pressure.

A standby condensate booster pump starts automatically when low pressure is sensed at the feedwater pump suction. Running feed pumps also trip automatically after a 45-second delay if the feed pump suction pressure is between 190 and 210 psig or after an 18-second delay if the feedwater suction pressure is below 190 psig. If the feed pump suction low pressure occurs after a main turbine trip, the feedwater level control valves (LV-10s) will automatically close to the 70 percent open position. Similarly, condensate booster pumps will trip if condensate booster pump suction pressure is less than 38 psig.

The A feed pump was out of service for required chemistry sampling when the event occurred. At that time, all three condensate pumps, two condensate booster pumps, and the remaining two feedwater pumps were running. A third condensate booster pump was in standby.

The loss of the UPSs and turbine trip at 5:48 a.m. affected the feedwater and condensate systems in a number of ways. The feedwater level control valves (LV-10s) locked up "as is," by design (at the approximate 100 percent flow position) because they lost their control signal with the loss of UPS 1B. Because of the turbine trip, these valves would normally have closed to their 70 percent open position. The minimum flow valves for the operating condensate, condensate booster, and feedwater pumps failed open as designed, upon loss of their control signals when UPS 1A and 1B were lost. The fourth point heater drain pumps tripped, by design, as a result of the turbine trip. The condensate demineralizer (2CNM-AOV109) and low pressure heater bypass valves (2CNM-AOV101) are designed to open automatically on a turbine trip at greater than 80 percent power to help control reactor vessel water level. These valves failed open as designed upon the loss of their control signal when UPS 1A and 1B were lost.

The opening of the condensate, condensate booster, and feedwater pumps' minimum flow valves, combined with the lockup of the LV-10s and the opening of condensate demineralizer and low pressure heater bypass valves, resulted in the condensate system going into a high flow condition approaching runout. A significant amount of flow to the suction of the feedwater pumps was either being diverted to the condenser via the condensate and condensate booster pump minimum flow valves or was lost due to the trip of the fourth point heater drain pumps. Similarly, the condensate booster pump suction flow was being diverted to the condenser by the condensate minimum flow valves. Low feedwater pump suction pressure caused the automatic start of the standby condensate booster pump and a trip (after an 18-second delay) of the running feedwater pumps. Low condensate booster pump suction pressure caused the automatic trip of one condensate booster pump when the standby condensate booster pump started. The automatic pump trips occur when the pump lacks sufficient water pressure to protect the pumps from damage.

Shortly after the loss of the five UPSs, the final status of the feedwater and condensate system was as follows: The feedwater pumps were tripped, and two condensate and two condensate booster pumps were running. Minimum flow valves were open and recirculating water back to the condenser hotwell.

At 6:11 a.m., the condensate booster pumps began injecting a large amount of water when condensate booster pump discharge pressure dropped below reactor vessel pressure with the LV-10s "locked up" open in their 100 percent flow open position. Operators initially tried to shut the LV-10s. When this was unsuccessful, they tripped the operating condensate booster pumps. Their response was hindered because the loss of the UPSs resulted in loss of a direct indication of feedwater and condensate system injection flow rates. Operators had indirect indication of flow by the feedwater check valves' position indication and inferentially from indicated increasing reactor water level. However, RCIC was injecting, so changes in reactor water level would not necessarily be caused by condensate booster pump injection. (See Section 5.3 for a further discussion of this condensate booster pump injection.)

With the control rod drive pumps providing the only source of injection, reactor vessel level was slowly decreasing toward the normal operating range. The operators wanted to restart a condensate booster pump to maintain reactor vessel water within the desired range. Feedwater and condensate operating procedure N2-OP-3 required that operators shut the feed pump suction valves (MOV-84s). The MOV-84s were required to be shut because of previous experiences at NMP-2 where the feed pump suction relief valve lifted and the suction relief piping was damaged because of air trapped in the system. After the start of the condensate booster pump, the MOV-84s in the injection flow path to the reactor vessel could not be opened because of the high differential pressure across the valves. The manual bypass valves for the MOV-84s could not be opened because the turbine building had been evacuated following restoration of the UPSs because UPS restoration had caused radiation monitors to spike and false alarm. (Had it been necessary, access to the turbine building could have been granted with radiation technicians escorting the operators.) Operators instead opened LV-137 (low flow/low pressure valve) from the control room and initiated condensate booster pump injection to the reactor vessel, bypassing the feedwater pumps.

The next significant problem encountered in the feed and condensate systems was the high stator winding temperature on the A condensate pump. The licensee suspected that this high stator temperature was caused by running the A condensate pump at a high flow rate. Operators started another condensate pump and a short time later the high stator temperature alarm on the A condensate pump cleared.

4.7 Other Systems

This section describes the operation of several systems which complicated recovery from the event. The partial loss of plant lighting and communications impeded recovery actions. The RCIC system experienced control and valve indication problems. The RWCU system tripped when put into service and may have experienced a water hammer. Operators experienced difficulty controlling an RHS throttle valve, which led to a reported water

hammer and high reactor water level alarms. In all cases, however, these problems were readily overcome.

4.7.1 Plant Lighting Systems

NMP-2 has five plant lighting systems: (1) normal, (2) emergency, (3) essential, (4) egress, and (5) 8-hour battery pack lighting. Normal lighting and the 8-hour battery packs receive power from normal ac power sources. Essential and egress lighting are powered from UPS 1C, and 1D, while emergency lighting power comes from Class 1E UPS.

Normal lighting refers to the lighting provided in all areas of the plant under normal conditions. Emergency lighting is provided in plant areas with safety-related equipment. Essential lighting provides partial lighting for areas with safety-related equipment. Egress lighting is provided for all areas leading to outside building exits. The 8-hour battery packs are provided in all areas that contain safe-shutdown equipment. Thus, those areas of the plant that contain safety-related equipment and safe-shutdown equipment, or that lead to outside exits include multiple lighting systems. The main control room, for instance, has normal, essential, emergency, and 8-hour battery pack lighting. The normal switchgear room where the nonsafety-related UPSs are located is served by essential and normal lighting systems.

The first reports of the event indicated erroneously that operators were without emergency lights, including those in the control room and other buildings. Confusion about the lighting occurred because operators and other plant personnel call the "essential lights" the "emergency lights." This confusion was subsequently clarified, but during the event, all lights powered from the essential lighting system were off.

In the route taken by the operator to make the initial UPS assessment, the corridor lights powered by the normal lighting system were on while those powered by the essential lighting system were off. Stairway lights were off because they are powered from the essential lighting system. Lights in the normal switchgear room were on, however, as the operators assessed the UPSs.

Some stairways have both essential and 8-hour battery packs lights, but these stairways were also dark since the 8-hour battery pack lights do not come on if normal ac power is available, as was the case during this event. In some areas of the reactor building, the lighting was also momentarily lost because the low-wattage high-pressure sodium vapor lights in the building go off when the power dips and require up to 2 minutes to come back on.

4.7.2 Reactor Core Isolation Cooling System

The reactor core isolation cooling (RCIC) system is a standby source of injection water for the reactor. The RCIC system consists of a steam-driven turbine pump and associated valves and piping (see Figure 4.30). The steam supply to operate RCIC comes from the B main steam line. The RCIC steam supply line is provided with automatic containment isolation valves. The RCIC pump is normally aligned with suction from condensate storage

tank A. RCIC suction automatically transfers to the suppression pool when a low level is reached in condensate tank A. The RCIC pump discharges to the reactor head spray nozzle. The RCIC flow controller is normally preset for 600 gpm. The RCIC injection line is provided with a motor-operated pump discharge valve and two testable check valves, ICS*AOV 156 and 157. A return line is provided for system tests or for running the pump in the recirculation mode as an aid to controlling pressure. A minimum flow bypass line to the suppression pool provides pump protection. RCIC automatically starts when water in the reactor reaches level 2 (the 108.8-inch level) and automatically stops when water reaches level 8 (the 202.3-inch level).

System Response and Problems Encountered During the Event

Immediately preceding the event, RCIC was in a standby configuration and considered operable. The system had one outstanding work order concerning flow oscillations observed at the last quarterly surveillance test. Subsequent to the work order, RCIC passed its quarterly surveillance test. Flow oscillations during the previous test were estimated to be approximately 30 gpm about a nominal 600 gpm.

The RCIC system was first used in the August 13, 1991, event at 5:55 a.m. when an operator manually initiated RCIC injection because of a decreasing reactor water level caused by the loss of feedwater and prior to the time operators used emergency operating procedures (EOP) to restore and maintain water level. The operator encountered RCIC flow oscillations of approximately 100 gpm. The operator then took manual control of RCIC and raised injection flow to about 700 gpm. Although the RCIC injection inboard testable check valve ICS*AOV157 initially indicated being shut, the operator determined that RCIC was actually injecting because the reactor water level stopped lowering and began to rise.

RCIC flow oscillations gave operators another problem to diagnose and handle at the beginning of the event. The initial impact of the false closed indication for check valve ICS*AOV157 was that operators did not have normal indication of RCIC injection using RCIC instruments. Operators rely on the check valves and flow indicator for positive indication of flow to the reactor vessel.

Operators reduced RCIC flow over the next several minutes as the reactor water level approached the normal band. About 6:14 a.m., RCIC injection was secured and the operator had established RCIC running in a recirculation mode. When the reactor water level exceeded 202.3 inches because of condensate booster pump injection, the RCIC turbine steam supply valve (ICS*MOV120) and RCIC pump discharge valve to the reactor (ICS*MOV126) both automatically shut. These valves automatically reopen if the 108.8-inch level is again reached, which will restart RCIC.

The next problem encountered with RCIC occurred at 9:37 a.m. when the system was declared inoperable because RCIC injection outboard testable check valve ICS*AOV156 did not indicate that it was shut. The RCIC pump discharge valve to the reactor (ICS*MOV 126) was isolated. (Technical specification Section 3/4.6.3 requires that the containment structure penetration be isolated within 4 hours.) Thus, RCIC was technically inoperable but restorable if needed.

4.7.3 Reactor Water Cleanup System

The reactor water cleanup system (RWCU) is designed to maintain reactor water quality by removing fission products, corrosion products, and other soluble and insoluble impurities. The system draws suction from the recirculation loop and from the bottom head of the reactor vessel; cools, filters and demineralizes that stream; and injects reheated coolant back into the reactor system by way of the feedwater system (see Figure 4.31).

The scram procedure requires that the RWCU be placed in "full reject" or that the operating RWCU pumps be tripped. This is because of a thermal stress concern for adding heated RWCU water to the cooler feedwater piping under low-flow post-scram conditions. Immediately following the scram on August 13, 1991, control room operators tripped the running RWCU pump. At 10:56 a.m., operators attempted to restore the RWCU to service to control plant chemistry and reactor water level. The system was to be operated in the full reject mode in accordance with the scram procedure. In the full reject mode, the RWCU discharge is directed to the condenser rather than to the feedwater piping. The normal steps for entering into full reject after a scram could not be accomplished since the RWCU pumps were not operating. Operators utilized procedure N2-OP-37, Section E.4, for RWCU pump start. When the pump started, the RWCU experienced high system differential flow between the water coming out of the reactor system and that going to the condenser. Actual flow was observed to be about 800 gpm to the condenser, whereas the operator starting the RWCU pump expected a flow rate of only about 100 gpm. Excessive differential flow above the setpoint started a trip timer. Operators attempted to throttle back the flow but the timer on the delta flow instrument reached the set time limit and the system isolated. Personnel in the RWCU heat exchanger room reported a water hammer and pipe movement when the pump was started that lasted for approximately 15 minutes. However, a subsequent walkdown of the system did not reveal any resulting damage.

4.7.4 Residual Heat Removal System

The residual heat removal system (RHS) at Nine Mile Point Unit 2 is multipurpose. It can provide low pressure coolant injection, containment structure spray cooling, reactor steam condensing cooling, suppression pool cooling, and shutdown cooling. See Figure 4.32. The shutdown cooling mode can be initiated when the reactor vessel pressure is less than 128 psig. It is used to complete reactor cooldown and maintain the reactor in a cold shutdown condition. Shutdown cooling is accomplished by drawing coolant from the A recirculation loop, pumping the coolant through heat exchangers, and injecting the cooled fluid into the reactor vessel. At NMP-2, the B RHS loop is preferred for shutdown cooling partly because it is equipped with an adjustable letdown valve to the radioactive waste tanks. At the time of reactor scram, the B and C RHS loops were tagged out of service for preventive electrical maintenance. Early in the event, the A RHS loop was activated in the suppression pool cooling mode to remove the heat added from the RCIC turbine exhaust. The B and C loops were returned to operable status by 8:10 a.m.

Early in the afternoon of August 13, 1991, operators were warming the B train in anticipation of shutdown cooling service. Warming involves draining reactor coolant through RHS piping and the heat exchanger to the radioactive waste tanks through valve MOV-142.

The procedure for RHS operation (N2-OP-31) states that MOV-142 should be opened to mid-position and then the upstream isolation valve MOV-149 should be opened. The procedure further states that if MOV-142 is opened fully, the possibility of steam flashing and water hammer exists. Electrical problems prevented MOV-142 from being opened from the control room and an operator opened the valve locally; however, local valve position indication is not available at MOV-142. When the warning system was initiated, plant personnel reported hearing water hammer noise. Systems engineering personnel subsequently walked down the system but found no damage and an investigation by the licensee indicates that the noise heard may have been the normal sounds of the pipes heating and expanding. The B RHS was at approximately 90 psig and the radioactive waste system was at essentially atmospheric pressure; therefore, high fluid velocity and fluid flashing should be expected. At 2:58 p.m., reactor recirculation pump P1B was shut down by procedure in preparation for putting the B RHS in service. RHS cooling was established at 3:08 p.m., when RHS pump P1B was started. Since RWCU was not operating, the drain line to the radioactive waste tanks was again utilized to control water level, with flow through the drain line being controlled locally. Operators experienced difficulty in controlling reactor vessel water level as the B RHS loop water entered the reactor, was heated, and underwent expansion. The high water level condition continued in the reactor vessel until about 5 p.m.

4.8 Time of Reactor Scram

Normally the signal generating a reactor scram is recorded on the control room alarm printer that is driven by the plant process computer. Since the plant computer was powered by UPS 1G, the signal which generated the automatic scram was not recorded. An automatic scram was known to control room operators and reported in control logs and interviews with the team by the following indications: 1. The scram solenoid lights on the control panel were energized, 2. The control room panels behind the front panel APRM indicators were downscale and LPRM downscale lights were lit, and 3. The scram discharge instrument volumes were full. An early automatic reactor scram generated from the turbine trip signal was indicated by the lifting of only 2 of the 18 main steam safety valves. By design, turbine trip produces the first input to the reactor protection circuitry producing a reactor scram. About 1 second later, high pressure in the reactor will also cause a scram signal to be generated.

To provide additional confirmation that NMP-2 scrambled early and automatically from the turbine trip signal, the event was modeled on the plant simulator. The simulation also predicted that only two safety valves would lift if reactor scram occurred from the turbine trip signal. When the simulation scenario was programmed to require a wait for the high reactor pressure scram signal, the additional power generation caused 11 safety valves to open with a peak reactor vessel pressure of 1100 psig, which is about 30 psi higher than the peak pressure that occurred during the event. Thus, the simulation confirmed that the turbine trip signal caused the automatic scram signal which scrambled the reactor.

Figure 4.1 Nine Mile Point unit 2 transformer yard

Figure 4.2 Nine Mile Point unit 2 main stepup transformers and isolated phase bus (IPB)

Figure 4.4 Offsite power system

NOTE:

1. ELECTRICAL INTERLOCK PERMITS CLOSURE OF ONLY THREE OR FOUR SWITCHES. ALL OTHER SWITCHES NORMALLY CLOSED.
2. THE TWO 345KV/115KV TRANSFORMERS ARE LOCATED IN DIAGONALLY OPPOSITE CORNERS OF THE SUBSTATION AND ARE APPROXIMATELY 400 FEET APART.

Figure 4.5 Simplified protective relaying sketch

Figure 4.6 2MTX-XMIB tank bulging

Figure 4.7 Oil cooler piping flange

Figure 4.8 2MTX-XMIB failed windings

Figure 4.9 Low voltage flashover point phase to phase

Figure 4.10 2MTX-XMIB high voltage tap changers

Figure 4.11 UPS power supply oneline

Figure 4.12 Voltage and current waveforms - 345kV system

Figure 4.13 Voltage and current waveforms - 115 kV system and RTXA

Figure 4.14 Voltage and current waveforms – 115 kV system and RTX8

Figure 4.15 Frontal view of a 75-kVA 1-series UPS unit

Figure 4.16 Simplified electrical single line diagram for a 75-kVA 1-series UPS unit

Figure 4.17 Card cage for 75-kVA 1-series UPS unit

Figure 4.18 Display panel for 75-kVA 1-series UPS unit

Figure 4.19 Simplified diagram for UPS control logic power supply (shown at time of event)

Figure 4.20 Simplified electrical single line diagram for safety-related 25-kVA 2-series UPS unit

Figure 4.21 Simplified block diagram for safety-related 25-kVa 2-series UPS unit

Figure 4.22 Reactor manual control system

Figure 4.23 Rod worth minimizer indication after a scram with power available

Figure 4.24 Nine Mile Point unit 2 control room layout

Figure 4.25 IRM/APRM recorder
IRM/APRM/RBM recorder
Indicating 100% as if UPS lost

Figure 4.26 Back panel 608 APRM status

Figure 4.27 Gaitronics paging unit

Figure 4.28 Post-accident monitor (PAM) for reactor pressure and level

Figure 4.29 Condensate and feedwater systems (simplified)

Figure 4.30 Reactor core isolation cooling system (simplified)

Figure 4.32 Residual heat removal system

5. HUMAN PERFORMANCE

This chapter describes and evaluates the response of reactor operators during the first half hour of the August 13, 1991, event at Nine Mile Point Unit 2 (NMP-2), when instrumentation and control were lost with the loss of the uninterruptable power supply (UPS) output power and when the stress and demands on operators were greatest. After restoration of the UPS, the scram recovery and progression to cold shutdown were normal. Equipment that malfunctioned during the event is identified in Section 3 and described in more detail in Section 4. This section describes initial operator response and provides the team's analysis of the significant actions taken by operators. The team also assessed the relevant operator training and the important procedures they used during the event.

As this event began, all control rods immediately and automatically were inserted in the reactor core in response to the reactor scram signal. However, operators lost control rod position indication. The team spent considerable effort examining what the operators did in this event and what they might have done for an actual anticipated transient without scram (ATWS) as they followed their emergency operating procedures.

Operators used symptom-based emergency operating procedures (EOP) in flowchart format developed from the Boiling Water Reactor Owners' Group (BWROG) emergency procedure guidelines (see Figure 5.1 and 5.2). NMP-2 EOPs are based on revision 4 of the BWROG emergency procedure guidelines and much of what is said here regarding EOPs is generic to other boiling water reactors. These guidelines are called symptom-based because they require that operators take actions to maintain or return multiple plant parameters to within specified limits. The governing philosophy of these EOPs is that the following three tasks be accomplished before operators address the specific cause of an event: (1) protection of the fuel cladding boundaries, reactor pressure vessel boundaries, and primary and secondary containment boundaries; (2) control of reactivity; and (3) maintenance of the heat sink (suppression pool).

The EOPs address key plant parameters, like the water level and pressure in the reactor vessel, as well as reactor power, and containment pressures and temperatures. The EOPs direct the operator how to respond to a parameter change or trend. They do not tell the operator the cause of the change. The EOPs use flowcharts to allow operators to follow the course of multiple parameters while easily keeping track of their position and the status of actions to be taken. Text-based procedures, on the other hand, would require that operators keep track of multiple procedures on multiple pages simultaneously. Prior to the Three Mile Island Unit 2 (TMI-2) accident, and for several years thereafter, the nuclear industry used event-based response procedures that were generally detailed, with specific procedures for specific problems. In a fast moving event, operators sometimes had difficulty in recognizing the cause of a condition and thus, sometimes did not use the appropriate procedure(s). The operators frequently used numerous, lengthy procedures, and sometimes had difficulty keeping up with the event. The symptom-based EOP flowcharts are a balance intended to ensure that the operator has sufficient, timely guidance. The effectiveness of the flowcharts depends on the training and knowledge of the operators to take appropriate actions with limited written guidance. Boiling water reactor (BWR) operators are trained that all EOP flowchart paths are equally important and that the parameters are interrelated (e.g., actions that affect reactor water level also affect reactor

pressure). In addition to using the EOPs for symptom response, the operators have event-based procedures to address component, equipment, or structure faults. These would include response to a scram, loss of feedwater or of annunciators, or a system otherwise operating off-normal.

5.1 Background to Licensee Procedures

The operations activities at NMP-2 are governed by many guidance and requirement documents, such as technical specifications, the site emergency plan, NRC regulations, and site management directives. The requirements and other guidance that govern operators are generally implemented by procedures.

One important class of operator response procedures are the symptom-based EOPs described above.

Other operating procedures used in the nuclear power industry are as follows:

- (1) general operating procedures, such as those for plant startup and shutdown that integrate and coordinate many activities and systems
- (2) system operating procedures that give directions for normal operation of a system and provide more detailed information than the general operating procedure for activities such as startup and shutdown of the system
- (3) off-normal (or abnormal) procedures for responding to specific plant events or operating system events, such as a pump trip
- (4) annunciator-response procedures for responding to individual alarms

The above procedures are typically text formatted, and event or situation based.

Specifically at NMP-2, "operations procedures" consist of some general operating procedures and some system operating procedures. The system operating procedures are written to continue (1) a system operating section, (2) an off-normal section, and (3) an annunciator-response section, corresponding to (2) and to (4) above, respectively, within each procedure. The "operations procedures" at NMP-2 are presented in a text format.

During an emergency, operators must also comply with emergency plan implementing procedures. These procedures implement the emergency plan and provide detailed guidance for emergency activities, such as event classification, notifications, activation of emergency response facilities, access control, damage control and protective active recommendations. These procedures at NMP-2 are presented in a text format.

General routine operations activities, such as log keeping, shift turnover, and control room conduct are controlled by operations department instructions (ODIs). Administrative procedures give guidance for activities, such as the use and control of procedures, equipment tagging, work order control, and administration of operation activities.

The team reviewed the procedures relevant to this event and evaluated their affect on human performance by considering the procedures' technical content, level of detail, format, clarity, consistency between procedures, and the transition or interaction among procedures.

5.2 Initial Operator Response

This section describes the conditions at the time of the event at NMP-2, including the instrumentation indications seen by operators, actions they took, and the important procedures they followed.

At 5:48 a.m., August 13, 1991, the shift personnel at NMP-2 were completing a routine night shift. The Station Shift Supervisor (SSS) and his assistant were in the SSS office (a partition within the control room), along with the Shift Emergency Planning Coordinator (SEPC) and his relief, who were performing shift turnover activities. (The SSS and Assistant SSS are both licensed senior reactor operators.) The Assistant SSS becomes the Shift Technical Advisor (STA) at any time that the crew begins using the EOPs. (The CSO and NAOE are also licensed reactor operators.) The Chief Shift Operator (CSO) was "at the controls area" and both Nuclear Auxiliary Operators "E" (NAOE) were out of the control room. The non-licensed "C" Nuclear Auxiliary Operators were at various locations outside the control room. A number of the on-coming crew members were at the site and on their way to the control room.

The first indications that the control room crew had of a problem was, in their words, when they heard a "popping sound." This was followed almost immediately by a loss of nearly all control room annunciators and all lights on the full core display, and an "eerie silence" in the control room, probably resulting from the loss of electrical equipment (see Figures 5.3 and 5.4). The crew at first thought that there had been some sort of power failure. Operators immediately checked many parameters, including electrical buses, reactor power, and reactor vessel water level and pressure. Control room panel 603 (P603) is at the center of the L-shaped main control boards and contains the full core display and many other instruments. (See Figure 5.5 for normal display at full power operation.)¹ Recorders on P603 had stopped and other instruments had failed either upscale, downscale, or as is (see Figure 5.6). The average power range monitors (APRMs) indicated 100 percent reactor power on this panel (Figure 4.25). All the computer screens were black (see Figure 5.7). Instrument indications were still available for motor and valve positions, breaker positions, electrical meters, and safety-related instrumentation. Emergency core cooling systems (ECCS) had both power and indication.

The first information available to the operators indicating that a reactor scram was required or had occurred was the following:

- (1) recirculation pumps downshifted (procedures require an immediate manual scram because of operation above the 100-percent control rod line).
- (2) Loss of all eight scram solenoid white lights, Figure 5.6 (they indicate that RPS solenoids are de-energized and that an RPS actuation is present).

¹ All photographs depicting control room displays were taken at the Nine Mile Point Unit 2 plant simulator.

- (3) Shift of post-accident monitor recorders to fast speed (which occurred at 1050 psig and exceeds the RPS high reactor pressure scram set point). (See Figure 5.8.)
- (4) Lighting of alternate rod insertion (ARI) initiation light (which occurred at 1050 psig reactor pressure). (See Figures 5.6 and 5.9.)
- (5) Downscale indication on APRM meters and LPRM lights on back panels (Figure 4.24), which indicate a scram had occurred. (See Figure 4.26).
- (6) Tripping of feedwater pumps.

The operators were quickly aware of these indicators. Other indications were available, such as the transfer of house loads that would normally indicate a turbine trip and reactor scram. Operators did not observe that two safety relief valves (SRVs) lifted and reseated at the time of the turbine trip and scram (a normal response to a turbine trip).

At this point, the Assistant SSS recommended a manual scram. The SSS concurred with the recommendation and the CSO turned the mode switch to shutdown, which generated a "backup" manual scram. Turning the mode switch to shutdown also automatically bypassed the closing of the main steam isolation valves (MSIVs) on low main steam line pressure.

About the time of the manual scram, 5:49 a.m., a non-licensed operator was assigned to monitor water level and pressure indications using the post-accident monitoring recorders at the ECCS panels and call out the readings while operators carried out manual scram procedures. IRMs were then inserted.

About 6 minutes after the manual scram, the SSS ordered the RCIC system started because reactor water level was decreasing. Operators encountered problems with RCIC speed and flow oscillations in automatic, so an operator took manual control by moving the RCIC flow controller switch (Figure 5.11) from automatic to manual. The RCIC inboard check valve initially indicated shut, but the operator determined that RCIC was actually injecting because reactor water level stopped dropping and began to rise when the operator raised RCIC flow to above 700 gpm to restore water level more quickly and as level returned to normal, RCIC injection flow was progressively reduced as the reactor's water level returned to near normal to stabilize it. Shortly after RCIC was started, "A" RHS pump was started in suppression pool cooling mode to remove heat that was being exhausted to the suppression pool from the RCIC turbine.

At this point, about 8 minutes had elapsed and, until this time, the operators were executing the scram portion of the shutdown procedure. When reactor water level indicated a reading below 159.3 inches — an entry condition for the reactor pressure vessel (RPV) Control section of the EOPs — the operators began using their EOPs. From that time forward, the operators used the EOPs in conjunction with system operating and off-normal procedures.

Shortly thereafter, operators left the reactor water level (RL) path in the RPV Control section of the EOP because rod positions could not be determined (although all rods were subsequently determined to be fully in) and the operators initiated steps in EOP C5 governing Level/Power

control (an ATWS contingency). Operators then inhibited the automatic depressurization system (ADS), as directed by EOP C5. At this point in the event, EOP concurrent requirements were: (See Figures 5.12 through 5.16.)

(1) Reactor Pressure (RP) path:

"stabilize reactor pressure below 1037 psig using the turbine bypass valves... [and] WAIT until all control rods are inserted to at least position 02 OR the reactor will remain shutdown without boron OR if boron is being injected, SLC [Standby Liquid Control] tank level drops to 900 gallons... OR the reactor is shutdown and no boron has been injected...."

(2) Reactor Power (RO) path:

"insert control rods using one or more of the following methods (EOP-6, Attachment 14)" and

(3) C5 contingency of Reactor Level (RL) path:

"using ONLY the systems below, maintain reactor water level between -14" [top of active fuel] to 202.3" and "WAIT until all control rods are inserted to at least position 02 or the reactor will remain shutdown without boron."

The "systems below" are listed as the control rod drive (CRD), RCIC with suction from the condensate storage tank, and feedwater and condensate. There is also an ongoing caution that "raising injection flow rapidly may induce a large power excursion and result in substantial core damage." See Section 5.4 for details regarding operator training on EOPs.

Concurrently, the SSS dispatched operators to the switchgear building and UPSs location to try to identify the cause of the loss of power to instrumentation and the computers. The SSS also declared a site area emergency (SAE) and began notifying both licensee personnel and government agencies. Because of the loss of the Unit 2 intercom communications system, Unit 1 control room operators were asked to announce the SAE over their plant page system. The SSS also assumed the duties as the site's Emergency Director (ED) and was responsible for both EOP implementation and overall site emergency response until he was relieved as the ED at 7:38 a.m.

At this time, the crew also had a variety of other tasks and concerns to contend with. They were evaluating how to keep the condenser available as a heat sink (such as directing whether to start the auxiliary boiler for steam seals, the mechanical vacuum pumps, and shutting the steam jet air ejectors, etc.). They also had to deal with fire detection concerns since the loss of the UPS units affected control room fire panel annunciation, so there was the potential need to implement in-plant fire watches. Operators had to identify which instruments were available and whether they were accurate, as well as performing post-scrum activities, conducting control room accountability tasks, dealing with the loss of communications equipment, assessing the importance of the loss of drywell cooling fans, and determining the status of the failed transformer that initiated the event.

Shortly after operators began using the EOPs, reactor water level reached a minimum at about 150 inches (Figure 3.6) and began to increase following RCIC injection. At this time, reactor vessel pressure was in the 900-1000 psig range. The SSS then read the EOPs as not allowing depressurization until control rods were verified as fully inserted and began to be concerned about making other sources of injection water available so that RCIC could be secured. Concurrently, he dispatched an operator to the local instrument racks in the reactor building to verify that the control room instruments being used were accurate.

Shortly after 6 a.m., an operator verified that IRMs were downscale on range 1. About 6:03 a.m., SRMs were fully inserted and began to indicate. This indication showed that reactor fission power was below the heating range. The team could not determine the precise time when the crew concluded that the reactor was shut down.

As pressure decreased, the RCIC operator was given successively lower pressure bands to maintain. As reactor pressure approached 700 psig, the reactor water level was being maintained at about 180 inches (approximately normal level) in anticipation of the reactor water level decrease that would occur when RCIC injection was stopped to limit further depressurization.

Almost immediately thereafter the SSS became concerned that the condensate booster pumps would inject because reactor pressure was approaching their discharge pressure. However, the water level was still increasing, an indication that the booster pumps were already injecting. The team determined from strip chart recordings that condensate pumps were injecting at this time. RCIC was configured in a recirculation mode rather than an injection mode. At that point, the SSS directed that the feedwater level control valves (LV-10s) be shut. Because the LV-10s were locked at their 100-percent flow position due to the loss of the UPSs, they could not be closed. (Operators were uncertain whether the booster pumps were injecting, although in interviews, an operator stated that the feedwater flow check valves showed intermediate position about this time.) The SSS also directed that the condensate booster pumps be tripped. During the approximately 4 minutes of condensate booster pump injection, the reactor water level increased from approximately 180 inches to greater than 202.3 inches (off-scale high) and reactor pressure decreased from approximately 670 psig to approximately 620 psig (see Section 4.6 for further discussion). Pressure continued to decrease to about 560 psig as the cooler water from the booster pump injection was heated in the reactor vessel. RCIC automatically stopped, as designed, when the reactor water level exceeded 202.3 inches. The reactor water level increased about 15 inches per minute for 4 minutes, so the maximum reactor water level reached was about 240 inches, about 1 foot below the main steam lines. The team estimates that the condensate booster pump injection rate was approximately 6000 gpm.

Shortly thereafter, the UPSs were restored and the remainder of the event, other than for verifying at 7 a.m. that control rods were indeed inserted, was a routine plant shutdown and cooldown.

5.3 Assessment of Operator Actions

In this section, key operator actions are assessed for their timeliness and appropriateness, as well as for the human performance factors that influenced the actions taken. Among the factors affecting operator performance are the plant indications available to them, their procedures (including the clarity, technical adequacy, layout, and ease of use of instructions), prior training, amount of time available to take an action or observe an indication, number of other competing actions and their priorities, crew teamwork and communications, and the physical arrangement of the control room panels.

Manual Scram

Initiating manual shutdown procedures was required by plant procedure AP-4.0 and a good operating practice. Procedure AP-4.0 requires that license holders "shut down the reactor when the safety of the reactor is in jeopardy or when operating parameters exceed any of the Reactor Protection System setpoints and automatic shutdown has not occurred." Adequate indications were available for the operators to deduce that a scram was necessary and that the time frame of the manual scram (about 1 minute into the event) was reasonable.

Reactor Core Isolation Cooling Actuation

Operators based the decision to start RCIC on the observed trip of the feedwater pumps and the lowering of the reactor water level. RCIC was started about 6 minutes after the mode switch was placed for a manual shutdown and before operators began using the EOPs on low RPV water level.

Use of the ATWS Contingency

EOPs for reactor pressure vessel control posed the following ongoing exit condition in the reactor level flowchart path: "if all control rods are not inserted to at least position 02 AND the reactor will not remain shutdown without boron then ... enter [EOP contingency] C5, Level Power Control." Operators made the decision to leave the RL procedure and follow contingency C5.

The operators' decision to enter EOP C5 was timely and appropriate. They lost the rod position indication (RPS) and could not confirm that all control rods were fully inserted without rod position indication and, lacking the availability of a reactor engineer to assess conditions, the crew could not confirm that the reactor would remain shutdown without boron injection as it depressurized and cooled.

Depressurization

The EOPs recognize that there was a possibility the reactor could become recritical if all control rods were not inserted. The procedures in EOP C5 placed restrictions on injection sources and cautioned against a rapid injection of cold water. The EOP RP path directed that operators "stabilize" pressure until the reactor was determined to be shutdown. Once the reactor was

determined to be shutdown, EOP RP path allowed depressurization and cooldown, while allowing for the possibility that the reactor might go recritical, at which point operators were to terminate the depressurization. Meanwhile, because control rod positions were not known, the EOP RQ path directed that operators insert control rods by alternate methods and that operators are not to perform the scram procedure actions simultaneously.

With RCIC running and other steam loads, the reactor began to depressurize. As described above, the EOPs directed "stabilization" of reactor pressure and restricted injection sources to CRD, condensate and feedwater, and RCIC. The EOPs allowed the operators to maintain a very wide water-level band (-14 to +202.3 inches). However, the operators increased water level toward the normal band (180 inches), exacerbating the pressure decrease (see Section 5.4). The CRD system was operating and would not maintain water level by itself and the feedwater pumps were tripped as a consequence of the UPS losses. The operators did not restart feedwater pumps. Not starting them was the correct course of action because feedwater flow instrumentation was lost and the feedwater level control valves were "locked up" in about the 100-percent flow position. Had feedwater pumps been restored, they would have caused a rapid injection of water to the reactor vessel at a time when there was an on-going EOP caution not to do so. Thus, operating RCIC was necessary to maintain or recover reactor water level. However, RCIC's operation acts to depressurize the reactor, and with substantial plant steam loads, the reactor will depressurize.

EOP implementation is based on the principle that operators take action on all parallel flowchart paths so that one set of procedures is not given priority over any other. The operators, however, receive training and may be preconditioned to favor some actions over others. For example, operators are trained that keeping the core covered ensures adequate core cooling and that, in an ATWS, the main condenser is the preferred heat sink because suppression pool temperature is the parameter in the EOPs which causes boron injection to be required. Because the operators continued to keep water level high with the use of RCIC injection, the reactor continued to depressurize.

The team posed a scenario similar to the above to the licensee's operations and training personnel and gave them about a day to consider their expectations of the operators' response. They stated that their expectations were that operators would attempt to stabilize pressure by stopping unnecessary steam loads, initially securing RCIC, and then using RCIC sparingly to maintain a slowly dropping reactor water level. The operators' response during the event was different.

Declaration of Site Area Emergency

The SSS declared a site area emergency (SAE) at 6:00 a.m. (EST) based on recommendations from the Shift Emergency Planning Coordinator (SEPC) and the Shift Technical Advisor (STA). The SSS made this declaration in accordance with site procedure EAP-2 based on the emergency action level (EAL) of loss of all control room annunciators while a transient is in progress.

The team's evaluation is that the declaration of the site area emergency was timely and appropriate. A transient was underway and some communications equipment and significant

instrumentation were lost, including control room annunciators, computer systems, and the control rod position indication system.

Condensate Booster Pump Injection

The plant was depressurizing because of RCIC operation and other steam loads. Control rod position was still unknown. The on-going caution in the EOP's C5 procedure that "raising injection flow rapidly may induce a large power excursion and result in substantial core damage" remained. At that time, the only running large injection sources were the condensate booster pumps.

Tripping the condensate booster pumps or shutting valves in the flow path is an action that must be anticipated. Because of the large flow rate of the system, operators cannot wait to see the symptoms for injection, such as level increases or feedwater flow indications. Once the condensate booster pumps start to inject, it is too late for operators to prevent a large injection and a possible overflow of the reactor vessel. Similar events are not unusual and have happened twice before at NMP-2. (Sections 6.4.1 and 6.4.2.)

At 6:11 a.m., a rapid water injection by the condensate booster pumps occurred. Reactor vessel water level increased from about 180 inches to near the steam lines. The team identified several performance-shaping factors that contributed to the rapid injection by the condensate booster pumps: (1) the crew was busy, and in a time-sensitive and stressful situation; (2) some BOP instrumentation was lost, such as reactor water level instruments and feedwater flow instrumentation; (3) the SSS was busy because he was fulfilling responsibilities for the Emergency Director and directing EOP actions; and (4) the EOPS have multiple procedure paths with each leg giving guidance while having ongoing exit and wait conditions, and sometimes, an ongoing caution statement.

Initial Operator Panel Readings

The team's assessment is that the operators gained much valuable information when they initially scanned control room instruments. Operators stated that they did not at first notice that the safety relief valves had lifted because the associated alarms were not functioning following loss of the UPS units. Thus, the momentary open-valve position indication was not noticed, and the operating reactor pressure recorders had shifted to fast speed. The recorders show about 3 inches of paper and, with the recorder at high speed (4 inches per minute), the pressure transient and associated SRV opening at the time of the turbine trip and scram were obscured on the paper take-up roll in approximately 45 seconds.

Operators identified the lifting of the SRVs later in the event using the restored tail pipe temperature trend charts when control room activities were less demanding. These trend charts stopped when the UPSs were lost and resumed when power to them was restored.

5.4 Emergency Operating Procedures Training and Related Training

The team examined the training of the licensed and non-licensed operators by reviewing selected lesson plans on many of the systems and procedures addressed in this report and the training records of the crew on the night shift at the time of the event. The team reviewed training on the three major Emergency Operating Procedures (EOP) implementation points that operators considered in their response to the event: (1) directions to exit the RL flowchart leg to C5, the contingency procedure for ATWS; (2) the caution on use of injection water sources during the implementation of the contingency procedure; and (3) guidance to stabilize pressure in the RP path. The team also examined operator simulator and UPS training. This section concludes with general observations on the licensee's training program.

5.4.1 Emergency Operating Procedure Training

The team reviewed the EOP-related training material, the EOP Basis Document for NMP-2, the Plant-Specific Technical Guidelines (PSTGs) for NMP-2, and the BWROG Emergency Procedure Guidelines (EPGs), Revision 4.

Operators are trained that cautions identify the potential adverse consequences of certain plant conditions or actions. Cautions do not direct operators to take specific actions or limit the applicability of the actions specified. With this training, operator's should be aware that a caution has ongoing applicability, that it provides a warning, and that it is not a directed action.

Operators are also trained to keep the MSIVs open so that energy is removed during an ATWS through the main condenser to protect the primary containment structure. Likewise, the concerns for recriticality caused by the injection of cold water and for assuring water level control with an active injection source during a post-scrum response are emphasized in training material and in the EOPs themselves.

The team noted that the operators were trained on the importance of keeping MSIVs open during ATWS conditions. This facet of training helps explain why the operators did not shut the MSIVs to control pressure during the event, nor do they caution against this action. The EOPs do not specifically direct operators to shut the MSIVs for this event.

Operators are trained on the EOPs to respond to the following four conditions (all or in specific combinations) to determine the shutdown status of the reactor for current and future conditions.

1. "All control rods are inserted to at least position 02."
2. "The reactor will remain shutdown (under all conditions) without boron."
3. "Boron is being injected and SLC [Standby Liquid Control] level is 900 gallons (769 pounds of boron injected)."
4. "The reactor is shutdown without boron."

However, there are inconsistencies in the training or training materials for how operators can verify and implement these conditions.

- Operator training for the RP path uses three of the four shutdown conditions in the RP path so that operators can make the determination of whether or not to proceed with a controlled cooldown at less than 100° F/hr. In its explanation on this section, the training material for the RP path does not discuss condition 4. This condition was initially misunderstood by the SSS but was later corrected by the Assistant SSS during the August 13, 1991, event. By answering "yes" to any one of those conditions, the operator would reasonably conclude that it is proper to proceed with the cooldown. The EPGs, PSTGs and EOPs consistently address all four conditions.
- Operator training for the C5, the ATWS procedure of the EOPs, adds an exit condition from the EPGs that is not in the PSTG and EOP: "Wait until the shutdown/cooldown procedure is entered and level above 159.3 before exiting C5." This guidance is to assure that exiting C5 is not done prematurely. With this condition and shutdown conditions 1 and 2, operators are directed to stop using the procedure and proceed to cold shutdown in accordance with the training material. In contrast, the EOPs direct the operator to the RL path to establish normal operator water level.
- Operator training for the RQ path is that conditions 1, 2, and 4 are overriding conditions to exit the EOP path. This condition is reflected in the EPG. The PSTGs justified a deviation from the EPG to prevent premature exit from RQ and conflicting actions of the EOP and scram procedure. If conditions 1 or 2 are met, they are the basis to terminate boron injection and enter the scram procedure. However, condition 4 is not in the RQ path of the EOPs. Further, their training for the RQ path uniquely describes to the operators that condition 4 addresses the situation with a few control rods not inserted into the core.

The licensee collectively presented EOP training material to operators within the current two-year operator requalification cycle. All the related lesson plans were given during the recent implementation of Revision 4 of the BWROG EPGs (early 1991).

The team reviewed how training addressed the raising of reactor water level using RCIC while the pressure was not stabilized. The RP override step in the cooldown process is as follows: "If the reactor is not shutdown, then return to... ." The operator is trained that prior to initiating RPV depressurization, the reactor must be shutdown and the cooldown must be secured if the RPV cooldown could result in criticality. The operator is further trained that with the reactor not shutdown, any significant depressurization and associated cooldown will not be possible because the positive reactivity added during the cooldown will increase reactor power and ultimately generate more steam than can be removed. The training material does not address this as a conflict. This aspect of the training and the EOPs implied that preventing pressure from going low is not as important as preventing high pressure or the maintenance of reactor water level for adequate core cooling. However, a standard operating guidance on the BWR flowcharts is that there is no priority between major flowchart paths or legs of the EOPs.

"Stabilize" is not defined in any of the training or procedural documents. The training material states: "No RPV pressure control range is specified in this step to allow stabilization of RPV pressure at any point below the scram setpoint....If necessary augment pressure control with one or more of the following systems... RCIC..." which provides makeup and heat removal of the turbine. The EPGs indicate that stabilization is intended to maintain a pressure generally below the scram setting. How much below is left to the judgment of each licensee and ultimately to the operator. The intent of this step appears to focus on situations when pressure is tending to increase rather than decrease. Pressure is controlled in the context of keeping pressure from increasing and challenging SRVs. The operators were never faced with this situation in training, despite at least two precursor events at the facility.

5.4.2 Training on the Uninterruptible Power Supplies

The team reviewed UPS training for licensed and non-licensed operators because interviews suggested that: the knowledge to manually override the CB-4 breaker came about through experience only, and several operators knew how to manually override the motor operator for CB-4, but apparently only one person at the UPSs knew how. A number of operators claimed that licensee did not teach practical UPS training or that, if they had the knowledge on manually operating CB-4, they acquired it from experience, such as by participating in the startup program for NMP-2. The team's focus in this area was to ascertain the nature of the training in light of the operators' statements.

The team noted that the licensee enhanced the training material based on industry and site operating experience. The lesson plans have a note that procedures do not cover manually shutting the CB-4 breaker and that this method would be pointed out in the plant. Training records indicated that all licensed and non-licensed operators who initially responded to the UPS rooms during the event had received UPS training. The licensee acknowledged that there was a good possibility that the "hands-on" training was either not completed, only discussed in front of the panel, or simulated on a very limited basis because of the potential to interfere with plant operations. The auxiliary operator and licensed operator initial qualification cards call for simulation or performance of routine and infrequent operations of the UPSs. None of this training was so specific as to require the manual override of the CB-4 breaker.

5.4.3 Simulator Training

The simulator at NMP-2 had not been programmed to run the event of August 13, 1991. Before the event, plans were under development to simulate the loss of an UPS affecting the control room annunciators. Only after reprogramming the simulator could the event be simulated on a limited basis.

The simulator malfunction index does provide for isolated power board and instrument malfunction/failures. The team found that the simulator programming that provided for power board and instrument failures or malfunctions were for discrete failures rather than common—cause failures of multiple pieces of equipment.

The team also reviewed a sampling of the training and simulator scenarios used for the crew on shift during the event. In the scenarios related to the ATWS contingency procedure, training

used more severe accident scenarios than those experienced on the day of the event. One scenario most closely resembles the August 13, 1991, event with the apparent dilemma of the EOP of keeping both water level and pressure high. This was the scenario on the failure of the reactor protection system with eight control rods stuck out following a partially successful alternate rod insertion. This scenario also involved a loss of feedwater and use of RCIC, along with containment problems. However, this scenario has the instructor play out the reactor engineer's analytical conclusion that the reactor will remain shutdown, thereby permitting a reactor depressurization and cooldown.

Overall, the licensee presented many challenging EOP scenarios that used multiple failures and multiple flowchart legs of the EOPs simultaneously. Formal training on the loss of all annunciators was not possible with the current simulator configuration and apparently the operators were never drilled on the interrelated objectives of stabilizing pressure and maintaining reactor water level during a partial ATWS.

In summary, on the day of the event, operators actually saw a set of malfunctions, symptoms, and perhaps even partial scenarios that they observed individually during their training. The event caused them to integrate their previous experience and training.

5.5 Command, Control, Teamwork, and Other Issues

Crew Perceptions

The team solicited opinions from among the operators interviewed about how well prepared they felt they were for this event. The control room operators reported good command and control by the SSS noting, in general, that he was the calmest of all. The SSS attributed these qualities directly to the organizational structure of the EOP flowcharts. Most felt that the static simulator training was very useful in diagnosing the August 13, 1991, event. The continuous drilling on the EOPs was cited as contributing to their perception of a positive outcome to the event. Operators also stressed the benefits of teamwork and the recent focus on electrical transient training. On the negative side, operators commented on not seeing a complete loss of annunciators coupled with a reactor transient; a lack of practical hands-on experience with UPSs; and site access restrictions at a time when they felt their help was needed, yet were held up because of emergency and security plan requirements (referred by the team to NRC's Region I for resolution).

Command, Control, and Teamwork

Based on team interviews with on-shift crew members and the NRC resident inspector who were in the control room for much of the event, control room command and control, direction, teamwork, communications, and use of procedures at the start of the event was professional and appropriate. The stress level was high, but operators stated that they had confidence in their training and felt comfortable performing their actions and stepping through the EOPs.

The SSS directed EOPs and also acted as the Site Emergency Director. He was responsible for both directing the operators and overall site emergency response. The Assistant SSS assumed STA duties during the event. He maintained a "big picture" perspective and provided insight and guidance, including assistance in diagnosing the event, in the loss of the UPS, and in the decision to insert a manual reactor scram. The SEPC assisted the SSS in classifying the event and in completing event notification forms and notifications.

NMP-2 reported that they had plans for some time prior to the event to make control room organizational changes. When SEPCs become STA qualified, the control room emergency organization will have the Assistant SSS directing the EOPs, while the SSS becomes the Emergency Director, and the SEPC fills the STA function.

Crew Experience

During interviews with the operators on shift (the "A" crew) at the time of the event, the team learned that most of the licensed and non-licensed operators were relatively new to their assigned positions (i.e., qualified within the last 2 years). On average, the crew had 9.5 years of nuclear experience, 4.9 years on site, and 1.9 years qualified in their assigned position. The normal SSS for this crew was on vacation and the normal Assistant SSS was the SSS with a substitute assistant from a relief crew.

5.6 Other Facility Operating and Event-Based Procedures and Implementation

As a result of the initial event review, the team reviewed how well facility operating and event-based emergency procedures supported human performance. Where procedural deficiencies or shortcomings occurred, the operators, in general, used their experience and/or training to compensate.

5.6.1 Scram Procedure

As a result of this review, the team noted that a number of important post-scram actions taken by the operators were not detailed in the EOPs. The actions were in OP-101C "Plant Shutdown Off Normal," Section H.1, "Reactor Scram." A note directs operators to leave this procedure if a use-of-EOPs condition is met. At the beginning of the RPV Control EOP, the RQ path gave reactor shutdown conditions: 1. "All control rods are inserted to position 02" and 2. "The reactor will remain shutdown (under all conditions) without boron." Answering yes to either condition, the operator would be directed to re-enter the scram procedure and perform this procedure simultaneously with other flowchart paths of the EOPs. These conditions were the same (i.e., dependent on rod position indication) used in the decision process for entering C5, the contingency procedure for ATWS. Similarly, on the day of the event, the operator could not answer yes to either condition (on indication of an ATWS). Further, it appears that operators were trained to implement OP-101C scram actions simultaneous with entering EOPs. However, on the day of the event, the operators implemented their training instead of literally

following the direction of the RQ path and implemented the scram actions in part simultaneously with the EOPs.

The team observed that, for potential ATWS conditions, important post-scram immediate actions might not be accomplished because of the intentional lack of detail in the EOPs. These actions would be: driving in SRMs and IRMs; verifying that reactor power is decreasing on APRMs (in distinction to the EOP terminology of monitor and control reactor power); and verifying that the scram discharge vent and drain valves are shut; securing flow to the vessel before level 8 (202.3 inches), which may require tripping condensate booster pumps if reactor pressure drops below their discharge pressure. The scram procedure is really an event-based emergency procedure as defined in ANSI/ANS-3.2 1982² (to which NMP-2 is committed). The team found that the procedure does not segregate and make a distinction between immediate actions and supplemental actions, contrary to the format and technical content requirements of the ANSI standard. The beginning portion of the EOP guidance for RPV control does not assure that operators complete important scram actions for all scrams, ATWS included.

5.6.2 Loss of Annunciator Procedure

The team reviewed the off-normal section on the loss of all annunciators of procedure OP-91A, "Process Computer." This procedure contains some general instructions, such as stationing extra operators to continuously monitor panel indications and increasing the frequency of in-plant equipment inspections. The procedure contains limited guidance to restore annunciators. This procedure would be considered an event-based emergency procedure, as defined in ANSI standard ANS/ANS-3.2 1982.

In reference to that ANSI standard, the loss of annunciator procedure provides no anticipated automatic actions. In retrospect, as a lesson learned from this event, such action is appropriate for a loss of UPS 1A and 1B since their loss will cause a scram. Specified actions require instrument and controls personnel to assist in determining the cause of the loss of annunciators. Operators referred to the procedure but did not implement it because of the limited usefulness of the guidance that was provided.

5.6.3 Uninterruptible Power Supply Procedures

Instructions for operating the UPS are contained in procedure OP-71, "13.8KV/4160V/600V A.C. Power Distribution." Controlled copies of this procedure are kept in the 237-foot elevation normal switchgear room and the 214-foot elevation and were available to the operators who restored power to UPS loads.

Several non-licensed operators were dispatched to attempt restoration of UPS loads shortly after 6 a.m. They reviewed sections of OP-71 to identify applicable guidance, but were unable to identify the instructions applicable to the situation facing them. They found in the off-normal section (H 27.0) of this procedure a section entitled, "UPS 1-series restart after UPS failure trip/transfer to maintenance supply." In reality and as they concluded, this also was not

² "Administrative Controls of Quality Assessment for the Operational Phase of Nuclear Power Plants."

applicable because the first steps of the procedure assumed the maintenance supply CB-4 breaker was shut. Shortly thereafter, a licensed operator arrived at the UPS location and also determined that there was no procedural guidance directly applicable to their situation. The operators stated that while these sections were not directly applicable, they were the closest thing they had to a workable procedure.

As discussed in Section 4.4 of this report, CB-4 is a motor-operated breaker, with no obvious manual control provision. Therefore, operators did not initially attempt to close CB-4 manually. They were not successful in restoring power to UPS 1D using the procedure. One operator at the UPS recalled from previous experience working with a systems engineer that by lifting the motor operator, CB-4 could be manually operated. They remembered that by lifting the motor operator away from the breaker, the breaker could be manually closed if they reached behind the motor operator and pushed up on the breaker operating mechanism. They used this method to successfully restore power to the loads associated with UPS 1D; they restored power to the remaining UPS loads in a like manner.

5.6.4 Condensate Booster Pumps Operating Procedure

As discussed in Sections 3.3 and 4.6, at 6:15 a.m., the control room operators stopped all condensate booster pumps. Subsequently, they needed to restart a condensate booster pump to supply water to the reactor and did so using the applicable sections of procedure N2-OP-3, "Condensate and Feedwater System" for a normal startup situation. The team noted that startup procedures do not address quick restart of feedwater and condensate pumps under emergency conditions, an anticipated available water source required in the EOPs. At NMP-2, the feedwater pump suction valves were shut because of the normal startup procedures and could not subsequently be reopened when operators tried to restore reactor water level. The licensee determined after the event that shutting the feedwater pump suction valves was unnecessary for condensate booster pump restart during the event.

5.6.5 Use of Damage Control Procedures

The Emergency Director decided to restore UPS 1A through 1D and 1G to their normal alignments during the morning of August 13, 1991. This decision was based on a desire to establish the most reliable configuration possible for this equipment and to minimize the possibility of an additional power loss. The Emergency Director was also concerned about the UPSs loads being supplied by unfiltered maintenance power.

The damage control team of operators and the UPS system engineer were directed to restore the equipment to a normal configuration. Restoring the configuration required that the team carryout complex tasks not addressed by any available procedural guidance. The damage control team did so, eventually working from the system engineer's knowledge of the equipment because the applicable procedure was not adequate for addressing this situation. The licensee's emergency response organization did not develop written temporary instructions that would have provided a measure of control over the restoration activity, although restoration proceeded with limited success. For example, only UPS 1C and 1D could be restored to normal while other UPSs could not be restored for a number of reasons, one of which was repeated feeder breaker trips. See Section 4.4 for a discussion of other equipment problems.

The team evaluated the restoration of the UPS to normal operations. The restoration was directed by the Emergency Director and implemented by a damage control team. The Emergency Response Organization and the damage control team had very little understanding of what caused the initial loss of the UPSs. The restoration itself could have caused another electrical transient, perhaps again challenging the operators who were in a controlled cooldown situation. At the time, there was no apparent rush to restore the UPS. Moreover, the damage control team's activities were not procedurally controlled.

5.6.6 Reactor Core Isolation Cooling Procedure

At the point in the event when RCIC was started, operators had not yet begun using the EOPs. RCIC operating procedure OP-35, Sections F.2.0, "Manual Initiation," and F.3.0, "Manual RPV Injection," both caution that "this procedure is to be used only if RPV Injection is required by EOPs." The licensee stated that the reason for the caution is that RCIC is to be started manually only when RCIC operation is directed by the EOPs. The operator started RCIC a minute before reaching an EOP entry point.

5.7 Man-Machine Interface

This section tabulates the instrumentation and controls lost or affected by equipment failures, the difficulties this presented to the operators, and the compensatory actions they took.

Table 5.1 Man-machine interface following loss of UPS power output

Instrument Lost/Affected	Operator Action	Difficulty Operator Encountered
APRM Recorders at P603 indicating power at 100%	Read back panel APRM indication down scale and LPRM downscale lights	On loss of normal indication, the operator had to remember other locations for indication and determine which was correct
Full core, RSCS, RWM and four-rod position indication lost	Had no indication that the rods were full in	Operator entered the C5 EOPs (ATWS)
Level and Pressure on control room panel P-603	Used the PAM recorders for level and pressure on P601 (marked by red template)	Operators had to determine which instrumentation was lost and which was providing accurate information. If feedwater was used, operable level instruments were out of eye range of operators at the feed and condensate control station
Feedwater system	Had to determine which alternate water systems were available and which was most appropriate for maintaining level	Operator had to use RCIC to control level while in C5 EOP, which made it difficult to control pressure
RCIC flow controller became erratic	Took the flow controller from automatic to manual	Operator had to recognize the problem and correct it before the system tripped
SPDS	Used alternate indication in and outside the control room to gather the data	Operator had to manually gather the data and transmit it over the telephone to the TSC
Feedwater flow injection	Had to recognize and use the indication lights for the check valves to determine if FW/condensate injection	Operator was delayed in determining that condensate booster pumps were injecting

Table 5.1 Man-machine interface following loss of UPS power output (cont.)

Instrument Lost/Affected	Operator Action	Difficulty Operator Encountered
While raising RV level RCIC inboard check valve indicating closed	Determined RCIC injecting by RV water level increasing	Operator had to determine if RCIC was operating properly, with normal indication providing ambiguous information
After running RCIC, the outboard check valve indicated open	Determined inoperability and isolated system to maintain tech. spec. requirements for inoperable isolation function	Operator had to isolate a system he could use for level control later in the event
Alarm lifting of safety relief valves (SRV)	Operator failed to recognize SRVs were lifting because of loss of the alarm and the PAM recorders for pressure went into fast speed removing the indication of the SRV lifting about 45 seconds after the event initiated. SRV indication does not have a seal-in feature to show that individual SRV(s) have lifted.	Operations performed technical specification required surveillance on a lifted SRV about two hours late
8 scram solenoid lights out	Operators understood this to be an indication that a scram had been initiated	Although these lights are on a red template indicating that they are a PAM instrument, the operator had to determine if they were lost due to the UPS loss or due to the initiation of a scram

Table 5.1 Man-machine interface following loss of UPS power output (cont.)

Instrument Lost/Affected	Operator Action	Difficulty Operator Encountered
CR fire annunciation was lost for them	Operations/Fire Departments attempted to determine status of system	Operations/Fire Departments needed to determine status of system and implement any required fire watches
Plant page and in-plant radios lost communication	Operators in the plant had to report in person. Unit 1 was contacted to make plant page announcements. The sound- powered phone was not conveniently available	Control room phones were sometimes busy, delays/time lost, difficult to assign in- plant operators other tasks or to give guidance
PAM recorders shifted to fast speed	SSS assigned operator to call out reactor level and pressure	Difficult for operators to discern trends. Possible contributor to delay in recognition of condensate booster pump injection

④

15 14 13 12

2010/07/25

SEQUENCE	DATE	TIME	LOCATION	REMARKS
120				
121				
122				
123				
124				
125				
126				
127				
128				
129				
130

C5 LEVEL/POWER CONTROL

START

Place ADS logic inhibit switches in ON

Containment concern, lowered level

FIGURE C5-2
MINIMUM ALTERNATE
RPV FLOODING PRESSURE

Figure 5.2 C5 level/power control leg of emergency operating procedures annotated by Incident Investigation Team (reduced from original size)

Figure 5.3 Full core display, rod sequence control, and rod worth minimizer after UPS loss

Figure 5.4 Full core display indicating lights on panel 603 (partial)

Figure 5.5 Panel 603 indicating full power operation (before loss of UPS)

Figure 5.6 Panel 603 after loss of UPS

Figure 5.7 Control room following loss of UPS (generally showing lost instrumentation)

Figure 5.8 Post-accident monitoring (PAM) reactor pressure and level (one of two PAM recorders)

Figure 5.9 Alternate rod insertion (ARI) indication that initiation has occurred

Figure 5.10 Back panel 608 LPRM status

Figure 5.11 RCIC controls

RPV CONTROL

Figure 5.12 RPV control entry conditions of emergency operating procedures

Section RL

(A)

Monitor and control
RPV WATER LEVEL

- CAUTION:** An RPV water level instrument may be used to determine RPV water level only when:
- The hottest drywell temperature is below the RPV Saturation Temperature (Figure RPV-1), AND
 - RB temperature near instrument legs are below the RPV Saturation Temperature (Figure RPV-1, EOP-6, Att 28), AND
 - The instrument reads above the Minimum Indicated Level

MINIMUM INDICATED LEVEL	
Instrument	Level
Shutdown Range	200 in.
Upset Range	190 in.
Narrow Range	150 in.
Wide Range	25 in.
Fuel Zone	-155 in.

- Initiate any of the following which should have initiated but did not (EOP-6, Att 1):
- Isolations
 - ECCS
 - Diesel generators

While executing the following steps:

IF	THEN
All control rods are $\geq$ 01 inserted to at least position 02 AND The reactor will $\geq$ 01 remain shutdown without boron	Exit Section RL of this procedure and enter CS, Level/Power Control
RPV water level cannot be determined	Exit Section RL of this procedure and enter CA, RPV Flooding
Primary Containment water level and suppression chamber pressure cannot be maintained below the Maximum Primary Containment Water Level Limit (Figure RPV-10).	Inspective of whether adequate core cooling is assured, terminate core injection into the Primary Containment from sources external to the Primary Containment until primary containment water level and suppression chamber

Figure 5.13 RPV control for water level (RL) leg of emergency operating procedures

Section RP

Monitor and control
REACTOR PRESSURE

While executing the following steps:		
IF	AND	THEN
A high drywell pressure ECDS radiation signal exists (1.68 psig)		Prevent injection from LPCS and LPCI pumps not needed for adequate core cooling prior to depressurizing below their maximum injection pressures
Emergency RPV depressurization is anticipated	All control rods are retracted to at least position C2 OR The reactor will remain shutdown without boron	Rapidly depressurize the RPV using the main bypass valves irrespective of the resulting RPV cooldown rate
Emergency RPV depressurization is required	Less than 7 SRVs are open	Exit Section RP of this procedure and enter C2. Emergency RPV Depressurization
RPV water level cannot be determined	Less than 7 SRVs are open	Exit Section RP of this procedure and enter C2. Emergency RPV Depressurization
	7 or more SRVs are open	Exit section RP of this procedure and enter C4. RPV Flooding

any SRV
cycling?

Manually open SRVs until RPV
pressure drops to 950 psig

While executing the following steps:		
IF		THEN
Suppression pool temperature cannot be maintained below the Heat Capacity Temperature Limit (Figure RPV 8)		Maintain RPV pressure below the curve (Figure RPV 8) respective of the resulting RPV cooldown rate
Suppression pool water level cannot be maintained below the SRV Tail Pipe Level Limit (Figure RPV 9)		Maintain RPV pressure below the curve (Figure RPV 9) respective of the resulting RPV cooldown rate
Steam cooling is required AND Boron injection is required AND The main condenser is available AND There has been no indication of gross fuel failure or Steam line break		Exit section RP of this procedure and enter C3. Steam Cooling Open the MSIVs (or prevent MSIV closure) and reestablish the main condenser at a heat sink (EOP-6, At 10) Bypass IAS and deaerator RPV water level MSIV isolation instructs, if necessary (EOP-6, At 10)

FIGURE RPV-11
SRV OPENING
SEQUENCE

Subsize RPV pressure below 1037 psig using the main turbine bypass valves
c. Augment RPV pressure control with the systems listed below, if necessary

- SRVs ... ONLY IF suppression pool water level is above EI 192 ft
 - Bypass LOCA isolation interlocks and reopen IAS supply valves, if necessary (EAS-SON164, 165, 166, 164)
 - If the continuous SRV pneumatic supply is or becomes unavailable, place the control switch for each SRV in the AUTO position
 - Open SRVs in the sequence listed in Figure RPV-11, if possible

128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200

122
120
132
125
121
135
126
130
127
129
137
134

Figure 5.14 RPV control for reactor pressure (RP) leg of emergency operating procedures

Section RQ

Figure 5.15 RPV control for reactor power (RQ) leg

C5 LEVEL/POWER CONTROL

START

While executing this procedure:		
IF		THEN
RPV water level cannot be determined		Exit this procedure and enter C-4, RPV Flooding
All control rods are inserted to at least position 02 OR The reactor will remain shutdown under all conditions without boron		Exit this procedure and enter RPV Control Section RL at (A)
Primary Containment water level and suppression chamber pressure cannot be maintained below the Maximum Primary Containment Water Level Limit (Figure C5-1)		Regardless of whether adequate core cooling is assured, terminate injection into the Primary Containment from sources external to the Primary Containment until primary containment water level and suppression chamber pressure can be maintained below the curve (Figure C5-1)
EMERGENCY RPV DEPRESSURIZATION IS REQUIRED		
		Continue at (H)

Place ADS logic inhibit switches in ON

While executing this procedure:		
IF	AND	THEN
Reactor power is above 4% or cannot be determined	Suppression pool temperature is above 110°F	Continue at (I)
	AND	
	An SRV is open or opens	
	OR	
	drywell pressure is above 1.68 psig	RPV water level is above -14 in.

Normal level

CAUTION: Raising injection flow rapidly may induce a large power excursion and result in substantial core damage

Using DMLY the systems below, maintain RPV water level between -14 in. and 202.3 in.

- During boron injection, maintain RPV water level as close as practicable to a stable value. Do not restore level.
- With no boron injection, recover level slowly.

- Condensate / Feedwater
- CRD (OP-30, Section H.7)

CAUTIONS: -Operating RCIC below 1500 rpm may result in equipment damage

- Elevated suppression chamber pressure may trip the RCIC turbine
- RCIC with suction from the condensate storage tank.

*

• Deviate low RPV pressure isolation interlocks, if necessary (EOP-6, Alt 2)

IF	THEN
RPV water level cannot be maintained above -14 in.	Maintain RPV water level between -45 in. and 202.3 in.
RPV water level cannot be maintained above -45 in.	Continue at (H)

Figure 5.16 C5 level/power control normal level leg of emergency operating procedures

6 INCIDENT PRECURSORS

6.1 Industry Experience with Uninterruptible Power Supply Failures

Uninterruptible power supply (UPS) units are utilized in power generating plants, communications centers, industrial plants, computer centers, and numerous other locations where either the quality or the continuous availability of electrical power is important. Certain loads are adversely affected by either the momentary interruption of power or by power source fluctuations which may be produced by normal power system switching or transfer operations, load changes, or system faults. The justification for use of an UPS is that it will provide uninterrupted, quality, stable power to its loads during those times when the UPS normal and/or alternate input power source(s) are interrupted or are of poor quality. The UPSs minimize, if not eliminate, the effects of disturbances which may exist on the normal electrical distribution system on UPS-connected loads.

A properly selected and applied UPS can provide continuous, quality, stable power to its connected loads throughout specified credible ac power system interruptions or disturbances. The UPS accomplishes this by supplying its loads through an inverter which receives its power from a dc battery when the UPS ac input power source is either lost or degraded. The type of loads selected for UPS power should be those critical loads which (1) would be lost, damaged, or operate in an unacceptable manner if they were subjected to voltage or frequency variations outside pre-established limits, or (2) require a source of power when the normal ac system is unavailable, or (3) require a filtered source of power.

Occurrences involving UPS failures have presented problems for nuclear power plants for some time. In order to obtain a perspective of the extent and scope of past UPS problems, the team searched the Nuclear Plant Reliability Data System (NPRDS), the Licensee Event Reports (LER), and Sequence Coding and Search System (SCSS) to identify events or failures germane to the Nine Mile Point event. The team also reviewed several generic documents that provide information and recommendations concerning UPS design and maintenance.

6.1.1 Nuclear Plant Reliability Data System Information

NPRDS is a data base of engineering data and failure records for specific nuclear plant components that could have a significant impact on the safety and reliability of the plant. The data base is maintained by the Institute of Nuclear Power Operations (INPO) and commercial nuclear power plants submit data to NPRDS for the specified components and systems.

The data revealed that several hundred occurrences had been reported, although many of these did not result in a loss of power to the applicable UPS loads. The failure categories are not sufficiently specific to identify failures that could be considered precursors to this event. Therefore, the team requested a word search of the failure narratives to identify problems with control logic, control logic power supplies, and control logic batteries. The team used several different synonyms, related words, and phrases to identify applicable

failure records. This search indicated that a few of the reported failures were caused by a control logic power supply problem similar to that experienced in this event, including two failures of the internal logic power supply itself. However, there were no failures identified where the control logic batteries failed to perform as designed. The team identified no event precursors from its review of the failure cause data.

6.1.2 Licensee Event Report Data

The team's review of Licensee Event Reports (LERs) focused on identifying events where loss of UPS had resulted in significant consequences similar to those of this event. SCSS contains LERs prepared by power reactor licensees and submitted to the Nuclear Regulatory Commission (NRC). The NRC maintains this data base at Oak Ridge National Laboratory. This data base contains event sequence, causal, and temporal information. Events caused by nonsafety-related components are not necessarily reported in LERs.

The SCSS data base search identified hundreds of LERs that reported UPS problems. The data base was also searched to identify LERs that reported loss of rod position indication or loss of annunciators caused by UPS problems, as well as any UPS losses that suggested the possibility of common-mode or common-cause simultaneous failures of multiple UPSs. These searches did not identify all problems because these failures would not require LER reports at all plants unless additional problems also existed. However, since that is often the case for loss of an UPS, the team felt that a representative number of failures were reported.

Only one event was identified where a loss of an UPS resulted in the loss of most of the control room annunciators, but this event did not involve a scram. No losses of rod position indication associated with UPS failure were identified.

The LER data review for common-mode or common-cause simultaneous failures identified seven events. Two of these involved the automatic transfer of loads following loss of one UPS followed by failure of the UPS to which the loads were transferred. Two losses were caused by personnel errors related to removing the UPSs from service for maintenance. In three cases, inverter (a UPS subsystem) losses that resulted in a transfer of the loads to the maintenance supply were caused by voltage spikes on a shared dc bus.

Several LERs identified potential common-mode failures because of hypothetical harsh environmental conditions and, on several occasions, a single plant declared two UPSs simultaneously inoperable because of a loss of room cooling. However, no actual simultaneous failures have occurred because of environmental conditions.

Thus, no common-mode internal causes were identified to have resulted in simultaneous UPS failures prior to the Nine Mile Point event.

6.1.3 Previous Generic Reports and Documentation of UPS Failures

Information Notice (IN) 88-05, February 12, 1988, "Fire in Annunciator Control Cabinets," addressed the common features of similar events at three nuclear power plants. One shared

feature was that the applicable annunciator equipment was from a common manufacturer. A contributing cause was high temperature in the power supply cabinets. However, the IN also addressed the "lack of specific emergency procedures to address the complete loss of annunciator response system." The IN was not specific on what attributes of an emergency procedure ought to be reviewed other than the need to have an emergency procedure to address this situation. Prior to the August 13, 1991, event, the licensee reviewed the IN for applicability to NMP-2, and made some procedural enhancements. (Section 5.5 addresses the NMP-2 procedure for loss of annunciators.)

In December 1986, NRC's Office for Analysis and Evaluation of Operational Data (AEOD) performed a case study, "Operational Experience Involving Losses of Electrical Inverters" (AEOD/C605), that reviews 142 inverter failures that occurred over a 3-year period. The case study identified three potential failure mechanisms: (1) high ambient temperature and humidity; (2) electrical interconnects and physical arrangement of inverter components, and (3) voltage perturbations. The case study addresses common-cause failures, but it did not identify control logic or control logic power supplies as specific problems. This case study noted that voltage perturbations clearly have common-cause implications and may result in the simultaneous loss of inverters. The case study resulted in issuance of IN 87-24.

IN 87-24 suggested that licensees monitor inverter temperature and humidity. Licensees were to evaluate the input and output voltages during steady-state and transient conditions to assure that manufacturers' recommendations were being considered. Additionally, to minimize the number of personnel errors, the NRC staff suggested reviewing inverter training and inverter-related maintenance and testing procedures. IN 87-24 also suggested that licensees verify the appropriate sequence of steps to achieve the desired maintenance and testing goals.

In March 1990, the licensee reviewed IN 87-24 and other industry reports. After its review of the temperature and humidity issue, the licensee concluded that 8 of 10 NMP-2 inverters have redundant internal cooling fans. The remaining two units have natural convection cooling. These two units were loaded less than 30 percent of rated load, and the internal components were widely spaced to allow the free flow of air, thus preventing local high temperatures. The licensee identified UPS 1D as having an over-temperature condition because of lack of heat sink grease on the inverter's silicon control rectifier (SCR). With the SCR problem corrected, the balance of plant safety-related UPSs were to have weekly filter and fan inspections. In addition, UPS 1D was to be evaluated for electrical overloading. Later the licensee identified that UPS 1C and 1D were "running hot," with the actual load near the rated load capacity, and they were in the process of procuring new equipment at the time of the event.

After its evaluation of input and output voltages during steady-state and transient conditions, the licensee concluded that full load operational transients were applied to each unit during initial plant startup and testing. Testing performed during initial plant startup was much more rigorous than required to "weed out" those components that were weak and subject to "infant mortality." They concluded that no more evaluations were required.

The licensee stated that operating and maintenance procedures provided detailed guidance. They also identified a common-mode of inverter failure that was caused by operator error during the startup and shutdown of the units. To minimize this error, they provided guidance in the operating procedures and on inverter unit labeling to better clarify fault and alarm conditions. In addition, the licensee incorporated into its training a system engineer seminar that discusses unique inverter terminology, design characteristics, and trouble indications.

None of these reports pointed to searching for design errors or deficiencies. They all addressed maintenance in broad terms identifying age related components such as capacitors. None specifically identified control battery problems. The licensee's responses to the various INs were reasonable and, in general, adequate.

The team reviewed licensee and NRC staff actions in response to NRC Bulletin No. 79-27, November 30, 1979, "Loss of Non-Class 1E Instrumentation and Control Power Supplies During Operation," because the event of August 13, 1991, had some similarities in nature to the events described in that bulletin. (Appendix B contains Bulletin 79-27.)

On November 10, 1979, at Oconee Power Station Unit 3, there was a loss of power to a Non-Class 1E 120 V ac single phase power panel supplying the integrated control system and the non-nuclear instrumentation system. It resulted in control system malfunctions and a significant loss of information to control room operators. A technician working on the condenser hotwell level caused a loss of the feedwater and condensate systems. After the resulting reactor trip, an inverter failed to properly transfer because of blown fuses, which resulted in a loss of indication for systems used for decay heat removal and the addition of water to the reactor vessel and steam generators. After 3 minutes, an operator manually transferred the inverter power supply.

Bulletin 79-27 also very briefly described a 1978 event at Three Mile Island (TMI) Unit 2 (LER 78-021-03L) (NUREG-0600) in which reactor coolant system depressurization and safety injection occurred on a loss of a vital bus because of an inverter failure.

The three actions recommended in the Bulletin 79-27 are summarized below:

- (1) Review Class 1E and Non-Class 1E power supplies to safety-related and nonsafety-related instrumentation and control systems which could affect their ability to achieve a cold shutdown condition using existing procedures (described in the second recommendation below); and, as a result of this review, identify key information and proposed design changes along with schedules for implementing those modifications.
- (2) Prepare emergency procedures or review existing ones that will be used by control room operators, including procedures required to achieve cold shutdown upon loss of the above-noted power supplies; and the procedures should include: (1) diagnostics/alarms/indicators/symptoms resulting from the above review; (2) use of alternate indication and/or control circuits which may be powered from other Non-Class 1E and Class 1E instrument and control buses; and (3) methods for restoring power to the bus.

- (3) Re-review NRC's IE Circular No. 79-02, "Failure of 120 Volt Vital AC Power Supplies," to include both Class 1E and Non-Class 1E safety-related power supply inverters; and, as a result of this review, describe any modifications or administrative controls to be implemented.

The licensee's documented responses on Bulletin 79-27 focused on recommendations (1) and (3). This focus was essentially an instrument and control failure modes and effects analysis (FMEA) on each component/power supply bus that would be used to achieve cold shutdown (three paths provided). The analysis applied to both safety-related and nonsafety-related equipment and, in particular, to both Class 1E and Non-Class 1E inverters. The final report identified the systems required for cold shutdown, the equipment and instrumentation to those systems, the required ac and dc buses, and it assessed the hardware impact of the loss of those bus loads on achieving cold shutdown. The FMEA was a single-failure analysis and did not consider the combined effects of multiple failures nor was it required to do so by the bulletin. The NMP-2 event involved the simultaneous failure of five power supplies. The NRC staff accepted the licensee's responses in this area as documented in the NRC staff's Supplement 3 of the Safety Evaluation Report (SER) for the NMP-2 operating license. The licensee and the NRC staff met the intent of recommendations (1) and (3) of the bulletin.

NMP-2 shows the effects of losing UPS 1A: RCS recirculation flow controls fail as-is; control rods cannot be moved (scram still available); condensate and feedwater recirculation control valves shift to UPS 1B; turbine functions lost shift to small motor generator backup; and fourth point heater drain pumps control shift to UPS 1B. NMP-2 shows the effects of losing UPS 1B: RCS recirculation flow controls fail as-is; control rods cannot be moved (scram still available); feedwater flow control valves fail as-is; condensate and feedwater recirculation control valves shift to UPS 1A; and fourth point heater drain pumps control shift to UPS 1A. If UPS 1A and 1B fail, the feedwater pumps would trip and the reactor would scram, as occurred on August 13, 1991. The plant should not experience a plant transient requiring shutdown if either UPS 1A or 1B fails. (See Section 4 for the major electrical loads on the loss of UPSs.)

The second recommendation of Bulletin 79-27 addressed the development or review of existing emergency procedures for the operators to cope with the losses identified as a result of the above noted FMEA. Considering when the bulletin was issued, the team noted that the focus of this review would be on event-based off-normal procedures rather than on the current symptom-based EOPs. The licensee's response to the bulletin in 1979 noted the unavailability of these procedures because of NMP-2's pre-licensing status. They provided only a commitment to review the adequacy of plant emergency procedures (Niagara Mohawk letter dated January 17, 1986). The NRC staff SER did not address this open issue because this aspect of the bulletin action was not embodied in the scope of pre-licensing "confirmatory issue No. 24" SER (NUREG-1045, Original Issue, pages 1-18, 7-42, and 7-43). The team found that the scope of this issue included only the FMEA review and not the emergency procedure review. The results of the FMEA indicated the importance of UPSs 1A, 1B, 1C, 1D, and 1G. Procedural improvements were not made that could have avoided challenging operator performance in the restoration of power output from the UPSs on the day of the event.

6.2 Nine Mile Point Unit 2 Precursors to the August 13, 1991 UPS Failure

The team reviewed the licensee's operating experience to identify precursor events. The following events are pertinent to the event on August 13, 1991.

6.2.1 February 1990 Event

On February 15, 1990, during modification work on a circuit card of UPS 1A, a technician and an operator caused the momentary loss of the power output. They immediately manually closed the maintenance circuit breaker, thus restoring power to critical loads and keeping the plant on line. To perform the work, the operator transferred the UPS power output to the maintenance supply, de-energized the control logic power supply, and removed a circuit card board. After the technician completed the modification work, he re-inserted the circuit card board and the operator re-energized the control logic power supplies. The technician noticed that an abnormal indication of a trip signal was showing on the mimic display. The operator de-energized the control logic power supply and then re-energized it to see if the trip would reset but it did not. The control logic power supply was again de-energized by the operator and the circuit board was reseated into its slot. When power was restored to the control logic circuits, the CB-4 motor operator apparently received a false open signal and, with CB-3 open, there was a loss of power output from the UPS. Realizing that the loss of power to the loads had occurred, the technician immediately lifted the CB-4 motor operator and closed CB-4.

Meanwhile, in the control room, operators observed the following: the rod drive control system locked up; the full core display, accumulator trouble, scram pilot, and rod drift lights all came on; recirculation flow control valve "A" locked up; the safety parameter display system computer tripped; one-half drywell coolers were lost; and circulating water system bypass gate valves went to mid-position. Reactor power remained at 97 percent, apparently because of the quick restoration of power output from the UPS or because certain loads were on their alternate UPS 1B power at the time. The momentary electrical disturbance from UPS 1A was sensed by the RPIS and all of the full core display lights would come on in response to the intermittent loss of power.

Meanwhile with the logic power de-energized, the technician rechecked the proper seating of all circuit card slots in the UPS unit. With the CB-4 motor disconnected from the breaker, the technician re-energized the logic power and reset the logic trip signal. He reconnected the motor operator to CB-4 breaker and successfully transferred loads back to the UPS' normal power output.

Licensee personnel documented this event in an internal report of February 17, 1990, and they provided subsequent lessons learned from the event. These lessons dealt with: (1) supervisory control of nonoperator manipulations of plant equipment; (2) the correct operating procedure to adequately cover all startup and shutdown, including the re-energizing the UPS logic circuits; and (3) additional "hands-on" training provided for operations personnel on manipulating the UPS controls.

6.2.2 April 1989 Event (LER 89-14)

On April 13, 1989, NMP-2 declared an Unusual Event when it experienced a reactor scram caused by a turbine trip from a generator protective circuit relay actuation. The turbine trip initiated a fast transfer of station loads from the normal station service transformer to the reserve transformers. Switchgear 2NPS-SWG003 failed to transfer, resulting in a loss of the operating feedwater pumps. Reactor vessel level decreased to the Level 2 setpoint, initiating high pressure core spray and reactor core isolation cooling. Power to the feedwater regulating valves was lost, causing them to fail in an as-is condition. Reactor pressure decreased to the discharge pressure of the condensate booster pumps resulting in condensate booster pump water injection and reactor vessel overfill.

Further complications occurred later in the event when the remaining 13.8 kV source was de-energized by an operator error. The loss of systems from this error resulted in use of the reactor core injection cooling (RCIC) system to maintain reactor vessel water level and the steam condensing mode of the residual heat removal system (RHR) used to maintain reactor pressure. At this point of cooldown in the sequence, UPS 1D tripped because of an overload condition that had existed for some time. Normally, this would have resulted in the UPS maintenance supply assuming the UPS 1D loads. However, with the loss of the 13.8 kV power because of operator error, the maintenance supply was unavailable. Loss of UPS 1D resulted in a loss of approximately one half of the plant's paging system and a partial loss of the plant's essential lighting. Loss of the paging system affected communications with plant operators outside the control room. In response to the UPS loss, the plant reduced electrical loads on UPS 1D to reduce the possibility of an overload trip.

Because of the April 1989 event and other UPS problems, the licensee prepared in March 1991, a conceptual engineering package for replacement of UPS 1C and 1D. In June 1991, a load shed study was done for UPS 1C and 1D. The conceptual engineering package stated that the 75 kVA-rated units have been run for extended periods of time in excess of their load rating. There have been multiple trips on each unit because of internal heat caused by overloading. The licensee determined that each unit had undergone some heat degradation. The study determined which possible existing loads could be shed from UPS 1C and 1D.

6.2.3 NMP-2 UPS Reports to NPRDS

A review of the licensee's NPRDS reports indicated occurrences associated with both the Elgar UPSs and the Exide UPSs.

The occurrences involving of the Elgar UPSs were mostly caused by blown fuses associated with synchronization to the maintenance supply and they mostly occurred from personnel errors during bus transfers. These occurrences reduced the reliability of the UPSs until the fuses were replaced, because at the time the UPS could not transfer to the maintenance supply; however, normal UPS operation was unaffected and there was no loss of power to the UPS loads. One occurrence involved a trip with automatic transfer to the maintenance supply caused by overheating when a cooling fan failed. No loss of power to the loads occurred.

Previous occurrences with the Exide UPSs were attributable to fans and internal circuits. These resulted in UPS trips on over-temperature or other trip functions and automatic transfers to the maintenance supply without loss of the UPS-supplied loads.

NPRDS data show no previous NMP-2 UPS occurrences that resulted in loss of power to the loads. In addition, the data do not show any similarities to the failures that occurred on August 13, 1991.

6.2.4 Review of UPS Work Orders

A review of the maintenance work order records for the five 75-kVA 1-Series UPS units show that pre-event maintenance consisted primarily of air filter replacement, recording meter and alarm indications, removal of dust and dirt, and the application of heat sink grease to silicon control rectifiers. There has been no maintenance for the control logic power supply battery packs.

6.3 Industry Experience with Transformer Failures

Failures of equipment and components comprising the electrical distribution system within the plant may or may not cause a unit trip, and in most cases are not expected to cause an extended unit outage. On the other hand, failures of equipment and components comprising the main power transport circuit from the generator to the 345 kV generator circuit breakers are expected to cause a unit trip and, more importantly, usually can be expected to cause an extended unit outage. For this reason, equipment and components which comprise this system need to be highly reliable in order for the plant to meet its design and economic objectives. Nevertheless, some components in the main power transport circuit have proven to be more susceptible to failure than others. The main stepup power transformer has proven to be unreliable enough that some utilities have hedged against their failure by purchasing and in some cases installing spare transformers.

At NMP-2, the unit main stepup transformer arrangement consisted of three single-phase main stepup transformers with an installed spare. With this design, the low voltage isolated phase bus system was connected to all four transformers when installed, with the bus conductor to the spare transformer disconnected but able to be connected into any one of the three phase positions simply by connecting the installed low voltage bus of the spare transformer in the correct phase arrangement. The transformer high side circuit arrangement also was designed such that the spare transformer high voltage bushing could easily be connected to any one of the three single phase overhead 345-kV lines that connect the transformer to the 345-kV Scriba switchyard.

Failure data for large power transformers have been published in IEEE 500-1984.¹ For the particular voltage rating and type of transformer which failed at Nine Mile Point Unit 2, the data from IEEE 500-1984 indicate that the best estimate of catastrophic failure rates for single-phase, liquid-filled, generator main stepup transformers in the 243-346 Kv class is once in 475 years (i.e., 0.24 failures in 1,000,000 hours), with low and high failure rate estimates ranging from 181 years (i.e., 0.63 failures in 1,000,000 hours) to 1280 years (i.e., 0.089 failures in 1,000,000 hours). Failure rate data from other sources were not available.

A review of LERs issued since 1988 indicates that there have been at least two other nuclear station main stepup transformers included in the same IEEE 500-1984 classification as the transformer at NMP-2 reported to have internal faults. In addition, there were at least six other nuclear station main stepup transformers reported to have internal faults which have different IEEE 500-1984 classifications than the NMP-2 main stepup transformer.

Information from the LER reporting network alone is insufficient to develop statistically significant failure rate data for comparison with the data contained in IEEE 500-1984. The team's LER search was restricted to transformers with catastrophic failures caused by internal faults. Of the eight transformers identified in this restricted category, two involved single-phase transformers similar to the NMP-2 transformer, and the other six involved three-phase transformers. Of the two single-phase transformers that have failed previously, one failed in January 1988 at Grand Gulf Nuclear Station Unit 1 and was manufactured by Westinghouse, and the other one failed in November of 1988 at Clinton Nuclear Power Station and was manufactured by General Electric. The transformer that failed at NMP-2 was manufactured by McGraw Edison. At Grand Gulf, Clinton, and at NMP-2, the licensees had a spare transformer of the same type and manufacturer as those that failed.

6.4 Industry and NMP-2 Experience with Overfilling Reactor Vessels

The licensee reported three events that involved overfilling reactor vessels. They are described in Section 6.2.2 above, and in LERs 86-020 and 88-001, described below.

6.4.1 Licensee Event Report 86-020

This event occurred while the reactor was in cold shutdown. A personnel error by electricians replacing a relay resulted in a division I emergency core cooling system (ECCS) initiation. One low pressure core spray pump (LPCS) and one low pressure coolant injection (LPCI) pump started and injected to the vessel. Both pumps injected for about 17 seconds before the operators placed the pumps in "pull-to-lock". Reactor water entered the main steam lines.

¹ IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations.

6.4.2 Licensee Event Report 88-001

The reactor scrammed from 41 percent power upon a loss of feedwater. The event was initiated when an operator isolated the air compressors while hanging a tagout. Instrument air pressure decayed to the point where the minimum flow valves for the condensate, condensate booster, and feedwater pumps failed open, which resulted in reduced feedwater flow to the reactor vessel. In an attempt to restore reactor water level, an operator placed feedwater control in manual and opened the feedwater level control valves. Feedwater pumps B and C and condensate booster pump B all tripped. The reactor then scrammed because of the lower water level. The water level continued to decrease and HPCS and RCIC automatically started at Level 2. HPCS was secured by operators at 195 inches and RCIC automatically stopped at Level 8.

Because of the low decay heat levels and the injection of cold water from HPCS and RCIC, the reactor depressurized. Approximately 5 minutes later, the feedwater minimum flow valves reclosed and the condensate booster pumps began to inject through the full-open feedwater level control valves. An operator attempted to close the feedwater level control valves but the valves locked up at approximately 80 percent open. Operators determined that feedwater was still injecting and then closed the feedwater containment isolation valves. Reactor vessel water level peaked at 333 inches (the bottom of the steam lines is approximately 252 inches).

The licensee's safety analysis of the event was that the effects of the main steam line flooding were within plant design margins. One of the corrective actions taken was to add a caution to the normal operating procedure to alert operators to monitor reactor water level continuously if the feedwater regulation valves are in manual.

6.4.3 Summary of NMP-2 Reactor Overfill Events

The licensee had two significant precursors due to the rapid injection by the condensate booster pumps (LER 89-014 and LER 88-001). NMP-2 corrective actions were taken to enhance procedures and training, and were not fully effective in preventing a recurrence of these events in that uncontrolled condensate booster pump injection recurred.

6.4.4 Industry Reactor Overfill Events

Only six boiling water reactor (BWR) overfill events were reported between 1980 and 1988 (AEOD Engineering Evaluation AEOD/E801). Four of the six events in the study occurred at BWR-5s (including the 1988 NMP-2 event). There are relatively few BWR-5s and they have been operating for less time than the earlier vintage BWRs. Even without the 1989 and 1991 NMP-2 events, BWR-5s dominate these type of events. The study stated that BWR-6s did not appear to be as susceptible to these events because of some combination of Level 8 trip of reactor feedwater pump discharge valves or condensate booster pumps. BWR-4 and older designs do not have RCIC spray into steam space and pressure reduction in response to RCIC operation is slower in these units. The AEOD study indicated that continued operator training, improved procedures, and perhaps hardware changes are necessary to completely eliminate overfill events. No generic communications from the NRC staff resulted on this study as of August 13, 1991.

7 REGULATORY REQUIREMENTS

The root causes of the loss of uninterruptible power supplies (UPS) at Nine Mile Point Unit 2 (NMP-2) were common-mode design and common-cause maintenance deficiencies. The design deficiency was the selection of the maintenance power supply as the preferred power source of the control logic power supplies instead of the inverter output power. The maintenance deficiency was the licensee's failure to periodically replace the UPS internal control logic power supply battery packs. Both deficiencies were undetected during unit operations. The loss of the UPSs caused loss of instrumentation and controls and information systems in the control room, and a concurrent plant transient, and unnecessarily and substantially challenged the operators.

The licensee classified the UPS 1A, 1B, 1C, 1D and 1G as nonsafety-related equipment. Their treatment of these was clearly different than the safety-related UPS 2A and B. The team made the following observations:

- The safety-related UPSs were lightly loaded and had internal temperatures that were cooler than some of the nonsafety-related UPSs that were heavily loaded and had internal temperatures that were hotter.
- The safety-related UPSs had controlled technical manuals and drawings. The nonsafety-related UPSs technical manuals and drawings were not controlled in the same manner as the manuals and drawings for the safety-related UPSs. (The manual contained inconsistencies that are discussed in Section 4.3.6 of this report.
- The safety-related UPSs had extensive preventive maintenance, including the planned change-out of internal capacitors, while the nonsafety-related UPSs had only routine preventive maintenance, such as filter change-out.

In the area of design, maintenance, and vendor interface, this treatment was different, as discussed in Section 4.3.6 of this report.

Accordingly, the team examined Nuclear Regulatory Commission (NRC) staff actions to regulate nonsafety-related equipment focusing, in particular, on the staff efforts to extend equipment classification and associated commensurate treatment to nonsafety-related equipment. The NRC staff issued Generic Letter (GL) 83-28, "Required Actions Based on Generic Implications of the Salem ATWS Events" on July 28, 1983, following a common-cause maintenance deficiency of the Reactor Protection System (RPS) trip breakers. The focus of the letter was to enhance treatment of the RPS equipment. The letter also described enhanced safety-related and nonsafety-related equipment classifications and treatment measures, including equipment vendor-licensee interface and the associated plant configuration management programs. Because of this, the letter was germane to the treatment of the UPS by the NMP-2 licensee and the NRC staff.

Further, loss of UPS 1A and 1B output power at NMP-2 was synonymous with loss of power to a non-class 1E instrument bus. Class 1E is defined in IEEE Standard 308 for safety-

related electrical systems. The NRC staff addressed this issue in Bulletin 79-27 "Loss of non-class 1E Instrumentation and Control Power Supplies During Operation."

The loss of control rod position indication and some neutron flux monitoring equipment complicated the event at NMP-2. For these instruments, the NRC staff identified applicable quality standards and attributes in Regulatory Guide (RG) 1.97 "Instrumentation for Light Water Cooled Nuclear Power Plants and Environs Conditions During and Following an Accident."

The team reviewed licensee and NRC staff actions on these issues. With respect to this event, the regulatory actions associated with GL 83-28, along with Bulletin 79-27 and RG 1.97, were considered by the team as they might apply to a programmatic treatment in preventing the loss of power to control room instrumentation and control systems.

7.1 Regulatory Classification of Equipment at Nuclear Power Plants

The team reviewed Commission and NRC staff actions on equipment classification and treatment. Based primarily on NRC staff interviews and reviews of related position papers to the Commission on the subject, the team established the following historical perspective.

Since the early 1970's, with the issuance of 10 CFR 50 Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," the NRC staff required licenses to have a high level of control for safety-related equipment in such quality assurance areas as design, fabrication, purchasing, storage, maintenance, operations and testing, etc. The term safety-related appeared to be well understood by vendors and licensees. Safety-related equipment ensures the integrity of the reactor coolant pressure boundary; the capability to shutdown the reactor and maintain safe shutdown; and, the capability to prevent or mitigate the consequences of accidents which could result in offsite radiation exposures comparable to guidelines in 10 CFR 100. The term "important to safety" is also used in the regulations, sometimes synonymously with safety related, and sometimes in a context subject to a broader interpretation.

Licensees and the NRC staff did not ignore the balance of plant (BOP) equipment (termed "nonsafety related"), and, accordingly, they purchased high quality commercial-grade BOP equipment. In some applications, there were no hardware differences between BOP and safety-related equipment. In some cases care and maintenance is very extensive (e.g., turbine generator).

Over the years, the NRC staff began to recognize the importance to plant safety of certain BOP equipment and broader classification of equipment termed "important to safety" and associated commensurate treatment. This broader classification included safety-related and important BOP equipment. This equipment was considered important because many plant transients were caused by BOP equipment malfunctions or failures and some BOP equipment provides redundant and diverse functions, either backing up or preventing unneeded challenges to safety-related systems and the operators. Use of the term "important to safety" when dealing with BOP equipment implied a three-level (or graded)

classification and associated treatment system: important to safety; safety related as a subset of important to safety (this overlap points to the lack of clarity of terms), and "nonsafety-related" or BOP equipment. Certain staff papers and documents to the industry refer to safety-related equipment as a subset of "important to safety" equipment. Meanwhile, some NRC staff and industry representatives of the industry used important to safety colloquially as a subset of balance of plant. Given those different usages, the issue was ripe for controversy.

The Three Mile Island Unit 1 (TMI) restart and Shoreham operating licensing hearings in the early 1980s established the NRC staff's endorsement of licensees developing the important to safety or graded approach concept. The staff reiterated that position in GL 83-28 in 1983. This evolving approach, coupled with the resolution of TMI actions items, gave rise to industry complaints that the agency was "out of control" and not affording them the opportunity of due process for equipment classification issues. Meanwhile, the industry assured the NRC staff that improvements in the treatment of BOP equipment were occurring and that the issue should be self-regulating under the auspices of such utility organizations as the Institute for Nuclear Power Operations (INPO).

In mid to late 1983, the Utility Classification Group, a group representing 30 electric utility owners of nuclear power plants, brought to the attention of the NRC Executive Director for Operations (EDO) what they thought was a matter of "major importance and increasing prominence" concerning internal NRC staff guidance and pending generic correspondence on this topic. The nature of their concern was that the staff was expanding the definition of safety related (with the use of "important to safety" terminology) without due process from the industry. They agreed with the NRC on the definition and regulatory basis for safety related. However, they cited examples in the regulations in which the terms "important to safety" and "safety related" were apparently used interchangeably while the NRC staff was defining important to safety in a sense that lacked a clear regulatory basis. The implication of this upgrade in classification was, in the industry's view, an upgrade in hardware qualification, perhaps to the highest qualification standards. In response, the NRC staff solicited the opinions of licensees on the topic in GL 84-01, January 5, 1984, which included the written views of the Utility Classification Group.

Further, in response to the group's challenge, the NRC's Director of the Office of Nuclear Reactor Regulation responded to the group on December 19, 1983. He explained in broad terms the differences between "important to safety" and "safety-related" and also provided the NRC's regulatory authority over "important to safety" equipment that was not "safety-related." The letter clearly indicated that the prescriptive requirements (treatment) of 10 CFR 50 Appendix B (Quality Assurance Programs) apply to safety-related equipment, but it fell short of stating what were the prescriptive requirements (NRC staff expectations) for the treatment of nonsafety-related equipment that was considered by the NRC staff to be "important to safety." The letter indicated that "requirements... allow the use of 'generally recognized codes and standards' where applicable and sufficient" for "important-to-safety equipment."

In an attempt to resolve this controversy following the Shoreham operating license hearing, in 1984 the Commission directed the NRC staff to prepare a rulemaking package. The

NRC staff prepared a position paper for the Commissioners, SECY-85-119, December 31, 1985 "Issuance of Proposed Rule on the Important to Safety Issue." The Commission unanimously disapproved the staff's proposed rule. The basis for the Commission's disapproval centered on residual unclear terminology and definitions. Instead, they issued a staff requirements memorandum for the staff to re-propose the rule and the Commission also provided the NRC staff with guidance to follow in proposing the new rule. This led to another staff position paper to the Commission, SECY-86-164, May 29, 1986, "Proposed Rule on the Important to Safety Issue." The basic issues described in this SECY paper were: (1) what equipment should be classified as "important to safety," and (2) what requirements are imposed on this class of equipment. The Commission did not issue a decision on this paper. The close-out memorandum of June 24, 1991, from the Commission Secretary to the EDO, indicated that the paper was being closed without Commission action "given the age of the paper."

Following these staff position papers, but prior to the close-out memorandum, NRC senior management provided the NRC staff guidance to avoid the important to safety terminology because of the confusion that it created. The confusion appeared to be centered on safety related being considered a subset of important to safety as well as with the interchangeable use of these terms in the regulations and other regulatory documents. However, the concern by the NRC staff about the treatment of BOP equipment remained because of its potential impact on safety. For example, an NRC inspection procedure reflects the staff's motivation and concern along with the related confusion on this concept. NRC Inspection Procedure 71500, September 30, 1988, "Balance of Plant (BOP) Inspection" is implemented at the discretion of NRC's Regional Administrators and involves the inspection of nonsafety-related areas. The guidance section states:

Developing issues with respect to BOP and presenting these to the licensee requires a different approach than for safety-related systems because of a shortage of prescriptive requirements. The basis for addressing BOP issues with licensees is that an aggressive, safety-conscious management approach will not be limited solely to safety-related hardware but will be reasonably applied to BOP systems that may cause challenges to safety systems at a relatively high frequency.

Other examples of NRC staff motivation on a graded approach to equipment classification, and associated attributes and treatment, appear in the discussion of RG 1.97, and in the discussion of hardware for conducting post-trip reviews and of vendor interface in GL 83-28. However, an example of a lack of clarity in existing regulations occurs in 10 CFR 50 Appendix B. The introduction and Section I indicate that: "the pertinent requirements of this appendix apply to all activities affecting safety-related functions." In contrast, Section II indicates that: "the quality assurance program shall provide control over activities affecting the quality of the identified structures, systems, and components, to an extent consistent with their importance to safety." The proposed rulemaking did not lead to a rule change to

reflect the NRC classification expectations as documented in the NRC Director's letter of December 19, 1983.

In reference to one aspect of the treatment of BOP equipment, on March 23, 1988, the Commission published a final Policy Statement on "Maintenance of Nuclear Power Plants," (53FR 9430). In it the Commission stated that it intended to publish a maintenance rule. The agency issued the final rule, "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," 10 CFR 50.65, on July 10, 1991 (56FR31306), along with the history of the development of the rule. Licensees are to implement the rule no later than July 10, 1996. The rule identifies the scope of the monitoring program to include structures, systems, and components that are safety related and certain nonsafety-related equipment. The term "important to safety" is not used. The rule is applicable to types of nonsafety-related equipment "that are relied upon to mitigate accidents or transients or are used in plant emergency operating procedures (EOPs); or whose failure could prevent safety-related structures, systems, and components from fulfilling their safety-related function; or whose failure could cause a reactor scram or actuation of a safety related system." Based on maintenance inspections, the rule was issued with the assumption that many licensees have fairly well established preventative maintenance programs applicable to nonsafety-related equipment.

UPS 1A and 1B are clearly within the scope of the maintenance monitoring rule. However, the rule alone, had it been issued 5 years earlier as written, may not have prevented this event. The monitoring rule would not require licensees to evaluate or change their current program until failures become apparent, thus indicating that the piece of equipment is not meeting its established goal for fulfilling its intended function. The rule does not address undetected faults, such as the UPS design or maintenance deficiencies revealed in this event.

7.2 Licensee and NRC Staff Actions in Response to Generic Letter No.83-28

The team reviewed NMP-2 licensee and NRC staff actions in response to GL 83-28, July 8, 1983, "Required Actions Based on Generic Implications of the Salem ATWS Events." (Appendix C contains a copy of Generic Letter 83-28.)

The letter addresses procedures and hardware to assure an adequate post-trip review; equipment classification for reactor trip systems and safety-related equipment; and, to a limited extent, the broader "important to safety" concept as it relates to vendor interface; post-maintenance testing; and reactor trip reliability. Clearly, the Salem anticipated transient without scram (ATWS) actions applied only to safety-related equipment and, more importantly, to the reactor protection system (RPS). However, the concept of vendor interface described in the letter is germane to the UPS losses. The letter also addresses the treatment of "important-to-safety" equipment. The vendor interface measures described in the letter could be viewed as a model for important BOP equipment.

Section 1.2 of the letter recommends actions associated with assuring sufficient and reliable hardware for conducting post-trip reviews. In this event, the licensee lost the plant process

and other computer systems because of the loss of an UPSs. In an NRC letter to Niagara-Mohawk of October 18, 1985, the NRC staff-endorsed review criteria stated in part that: "All equipment used to record sequence of events and time history information should be powered from a reliable and non-interruptible power source. The power source used need not be safety related." The NRC staff also asked the licensee to address power sources for such equipment at NMP-2. The NRC staff's supplemental SER No. 4, for the NMP-2 Operating License accepted the UPSs as a power supply for the process computer and other system computers. The loss of the plant computer removed an aid to the operator in analyzing plant conditions and reduced information that was available for the TSC or for a post-scrum review.

Section 2 of GL 83-28 addresses the enhancement of equipment classification and licensee/vendor interface for safety-related equipment (Sections 2.2.1 and 2.2.2 respectively), especially RPS equipment (Section 2.1). In this context, vendor interface guidelines were: for assuring that vendor information is complete, current, and controlled throughout the life of the equipment, and that this information is appropriately incorporated into plant instruction and procedures. Typical vendor information included vendor manuals and drawings, recommended maintenance and/or maintenance package service, extended warranty service plans, etc. These expectations were clarified in GL 90-03, "Relaxation of Staff Position in Generic Letter 83-28, Item 2.2 Part 2, Vendor Interface for Safety-Related Components," March 20, 1990. The NRC staff eased its position on having a vendor interface program for each safety-related component, accepting the use of the INPO-sponsored Vendor Equipment Technical Information Program (VETIP). The staff's intent was to ensure equipment reliability commensurate with its safety function in reference to 10 CFR 50, Appendix A, General Design Criteria (GDC) No. 1, "General Design Criteria, Introduction."

Section 2.2.1.6 of GL 83-28 also stated: "Although not required to be submitted for staff review, your equipment classification program should also include the broader equipment classification of structures, systems, and components 'important to safety' required by GDC-1." There was no specific NRC staff review criteria to judge the acceptability of licensee responses to section 2.2.1.6 of GL 83-28.

In a letter of April 10, 1984, the licensee responded that they were participating in the Utility Safety Classification Group seeking a generic resolution of the staff's concern about this broader class of equipment termed by the NRC staff "important-to-safety." stating, "We do not agree the plant structure and components important to safety constitute a broader class than the safety-related set. Nevertheless, we believe that non-safety-related plant structures, systems and components have been designed and are maintained in a manner commensurate with their importance." In its letter to the licensee of September 20, 1989, on GL 83-28 Item 2.2.1, "Equipment Classification Program for all Safety-Related Components for Nine Mile Point Units 1 and 2," the NRC staff endorsed the work of its contractor. The contractor stated: "...since the generic letter does not require the licensee to furnish this information as part of their response, this item will not be reviewed."

7.3 NRC Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power Supplies During Operation"

This bulletin was issued because of an event where loss of a nonsafety-related instrument bus caused a transient and loss of instrumentation in the control room challenging the operators ability to shut down the reactor. Section 6.1.3 of this report describes the actions taken by both the licensee in response to the bulletin and the NRC staff review of the licensee's actions. The licensee performed a failure modes and effects analysis (FMEA) of the loss of their UPS, taken one at a time. The FMEA was submitted to the NRC and reviewed and accepted by the staff. This analysis is, by its nature, structured so that faults are systematically addressed on a single-failure basis. The Bulletin recommends the development or revision of emergency procedures based on the FMEA.

In essence, this is an integration of engineering information into the emergency procedures, and it implies an integration to human performance and training. The licensee had no documentation of their emergency procedure actions, and apparently, the NRC staff did not ensure this action. The licensee's FMEA was not intended to analyze multiple simultaneous failures and their resulting effects on human performance, procedures, and training, which would be difficult to do. The FMEA identified many potential problems that were realized in the event of August 13, 1991.

7.4 Licensee and NRC Staff Actions in Response to Regulatory Guide 1.97

Control rod position indication and neutron flux monitoring were important instrumentation indications during the NMP-2 event of August 13, 1991. Because of the loss of all control rod position indication and loss of neutron monitoring equipment on the front panel during the UPS power outage, operators were left without certain information normally used for assessing safe shutdown of the plant. Regulatory Guide (RG) 1.97 addresses this instrumentation.

GL 82-33, Supplement 1 to NUREG-0737, "Requirements for Emergency Response Capability," issued in December 1982 incorporated into one document all the TMI related items approved by the NRC staff for licensee implementation. GL 82-33 provided additional clarification regarding the safety parameter display system (SPDS), detailed control room design reviews (DCRDR); RG 1.97, Revision 2; upgrade of emergency operating procedures, emergency response facilities, and meteorological data. The NMP-2 licensee committed to RG 1.97, Revision 3, by Final Safety Analysis Report (FSAR) Amendment 17. Their responses are included in a letter of October 5, 1984, and one of January 20, 1986.

RG 1.97 provides a method acceptable to the NRC staff to assure that minimum complement of instrumentation is available to monitor key plant parameters and systems during and following an accident. The RG defines various types of variables important to post-accident monitoring. Type A variables are essentially those needed for operator manual safety actions and Type B are essentially those needed to confirm the completion of safety functions.

Further, licensees are to assure the measurements and indications for these variables are of high quality and are reliably displayed in the control room, technical support center, and the emergency operations facility. Accordingly, the RG correlated variables (and types) to three prescriptive design and qualification criteria. Many of the instrument variables listed in the RG are not required to be redundant, and many are simply required to be high quality commercial grade powered by reliable power supplies. The RG characterizes these instruments as "important to safety." Some of them are safety-related and some are not.

In reviewing the RG 1.97 submittal by the licensee, the team noted that they did not provide detailed design information for each instrument. The NRC staff accepted the NMP-2 submittal without requesting important information, such as the specific power source to each component or subsystem. The NRC staff also accepted the licensee's list of type A variables without validation to the criteria in the RG.

On November 1988, the NRC's Region I conducted a RG 1.97 inspection of NMP-2. The inspection covered only eight variables and revealed only minor problems, mostly with instrument range indications. Because of the multitude of instruments at the facility, the RG 1.97 inspection amounted to only a spot check. The inspection was limited by the NRC staff's safety evaluation report (SER) for the licensee's acceptance of RG 1.97. The SER had accepted the licensee's interpretation of RG 1.97 for the Type A determinations.

RG 1.97, Revision 3, classified neutron flux (SRM and APRM) as a Type B variable and Category 1. Category 1 requires that equipment be Class 1E qualified among other qualification criteria. At NMP-2, the neutron flux system is made up of three overlapping monitor ranges. The important monitors for a unit scram are the APRMs and the SRMs. Table 4.10 provides the critical information about the neutron flux system. The system does not meet Class 1E criteria and is neither environmentally or seismically qualified. Reliable power is provided to some components from UPS 1A, UPS 3A, and UPS 3B. The SRMs and IRMs receive power from a reliable 24-V dc supply. The IRM and SRM drives receive power from normal 120-V ac. At the time of NMP-2 licensing, there was no Category 1 neutron flux equipment available for boiling water reactors (BWRs). The licensee originally committed to install a Category 1 system when available.

The NRC staff accepted a temporary exception to the staff position that power range monitors be Category 1. This issue received considerable industry and NRC attention in that the BWROG challenged the NRC staff's position on the need for this instrumentation to be fully qualified. In March 1991, the Director of the NRC's Office of Nuclear Reactor Regulation accepted the BWROG position, deferring further consideration to the ongoing severe accident management program. In their appeal, the BWROG placed reliance on the use of control rod position indication to verify reactor shutdown status.

RG 1.97, Revision 3, classified rod position indication as a Type B variable and Category 3. Category 3 equipment required no specific quality provisions. The source of the position information is the RPIS which includes the rod reed switches. The licensee only credits the full core display (provided information by the RPIS) as the RG 1.97 indicator. Table 4.9 provides the critical information about control rod indication. The system is not qualified to Class 1E criteria and is neither environmentally or seismically qualified. Reliable power

comes from UPS 1A with UPS 1B used as a backup to RSCS and RWM. However, since RPIS does not have a backup power source, the five display systems would be inoperable on loss of power to RPIS. On the day of the event, the lack of control rod position indication led the operator into the ATWS procedure. An actual ATWS condition did not exist.

During the event of August 13, 1991, control rod position indication was lost, and neutron flux was used to verify that the reactor was shutdown. Both neutron flux indication and the loss of control rod position indication were used by operators to make decisions as directed by the EOPs. With control rod indication unavailable for the critical first half hour of the event, operators used the ATWS procedures. Accordingly, the control rod position indication and neutron flux indications were key parameters as related to operator performance.

8 FINDINGS AND CONCLUSIONS

The event at the Niagara Mohawk Nine Mile Point Nuclear Station Unit 2 (NMP-2) began shortly before a shift change at 5:48 a.m. on August 13, 1991. It was initiated by an internal failure of the B phase unit main stepup transformer caused by a high voltage winding fault to ground. This failure resulted in automatic actions which isolated the faulted transformer and safely scrammed the reactor. The fault caused depressed voltages on the transmission grid and on the in-plant electrical distribution system until they were isolated from the faulted transformer. During the time that the in-plant electrical distribution system was connected to the faulted transformer, five of the ten uninterruptible power supply (UPS) units in the plant isolated themselves from their input power supplies and from their loads.

Their loads included some plant instrumentation and control loads which are normally available for control and status indication for the reactor, the loss of which, in conjunction with the ongoing transient, required a declaration of a Site Area Emergency. This event resulted in the initiation by the U.S. Nuclear Regulatory Commission (NRC) of an Incident Investigation Team on August 15, 1991 to investigate the incident. The findings and conclusions of the Incident Investigation Team follow.

8.1 Safety Significance of the Event

The event was of low safety significance and resulted in no actual adverse safety consequences.

- The event essentially involved a turbine trip, automatic reactor scram, and loss of feedwater, complicated by loss of instrumentation and control and a variety of equipment, as discussed throughout this report. The emergency core cooling system (ECCS) equipment available prior to the event remained operable, much balance of plant (BOP) equipment was available, offsite power and the emergency diesel generators remained available, and safety-related instrumentation was operable for reactor level and pressure, and for containment parameters. Neutron monitoring instrumentation was also available in the control room. The reactor automatically scrammed and reactivity control was provided by the automatic response of the reactor protection system (RPS). Containment integrity was also maintained throughout the event. Suppression pool cooling was used, safety grade containment cooling was available, and the automatic containment penetration isolation valves were operable.

8.2 Operator Coping With the Event

A significant aspect of the event lies in the challenge that it presented to the operators. The operators coped, but errors were made.

- The operators were required to take many high priority actions in a high stress, time-sensitive environment while many of their normal indicators,

alarms, and communications were not available or misleading. They determined which indicators were working and which were not, and obtained information elsewhere for those indicators that were not working, failed, or were contradictory or ambiguous with other indications.

- The Station Shift Supervisor (SSS) simultaneously filled two very demanding roles in directing both the Emergency Operating Procedures (EOPs) and overall Site Area Emergency.
- This event placed a high reliance on operator knowledge, training, and procedures.
- Operators diagnosed the instrumentation losses were UPS related and restored the UPS loads.
- Operators recognized that the reactor had scrammed or that a scram was needed, and manually scrammed the reactor as a backup.
- Operators used the appropriate EOPs. Because rod position indication was lost, operators entered the anticipated transient without scram (ATWS) EOP contingency.
- Operator actions did not prevent reactor depressurization prior to their verifying that the reactor was shut down.
- Allowing a rapid injection of cold water to the reactor while implementing the ATWS EOPs was a mistake, even though this event did not have actual safety consequences because the control rods were fully inserted.
- Although the operators were taking actions for a partial ATWS, the probability of an ATWS occurring was very low.

8.3 Transformer

The data available from the surveillance and maintenance records did not give any anticipatory warning that a failure of the transformer was imminent.

- The initiating factor for this event was the internal failure of the B phase unit main stepup transformer which sustained a high voltage winding fault to ground.
- A review of the periodic maintenance program that had been followed for the failed transformer with regard to inspection, testing, monitoring, and preventive maintenance practices, indicates that the maintenance program followed by the licensee is consistent with the state of the industry maintenance and surveillance practices.

8.4 Loss of Uninterruptible Power Supplies

The failure of the five nonsafety-related UPS was due to a common mode design deficiency and a common cause maintenance deficiency. Had either deficiency been corrected, the loss of the UPS would not have occurred.

- The design of the five UPS units are identical and hence all were vulnerable to the degraded voltage due to the transformer fault.
- Maintenance practices used for the five UPS units were identical. Internal control logic batteries had not been replaced in any of the five UPS and they were dead. Although being charged continuously, they degraded due to age.
- The UPS technical manual was inconsistent between its text and its drawing with regard to the power source for the internal control logic. The units were wired in accordance with the drawings, which shows the control logic connected to the maintenance supply as the preferred source. Since the event, the units have been rewired in accordance with the text, which states that the control logic should be connected to the inverter output as the preferred source.
- The technical manual did not clearly state the function or the importance of the control logic batteries.

8.5 Instrumentation and Emergency Operating Procedure Integration

The difficulty that operators experienced with loss of rod position indication during a transient had been underestimated.

- When the UPS failed in this event, the control rod position indication was lost, requiring the operator to enter the ATWS contingency procedures. In addition, control rod position indication is a key variable in boiling water reactor (BWR) EOPs for verification that the reactor will remain shutdown.
- The control rod position indication system is vulnerable to single failures such as the loss of a single UPS, which can cause a reactor scram and loss of control rod indication under certain conditions.
- NRC Regulatory Guide (RG) 1.97 ascribed no special quality or redundancy to the control rod position indication system, which the Guide considers as performing a verification function only.
- The NRC reviews of the licensee's EOP and RG 1.97 submittal were not fully integrated among the various disciplines within the NRC.

- The instrumentation with the highest RG 1.97 quality standards, such as pressure and level instrumentation, remained operating during the event and provided valuable information to the operators.

8.6 Emergency Operating Procedures Beneficial to Operators

The emergency operating procedures guided the operators and generally supported their decision-making process.

- Confronted with the losses of instrumentation and control and annunciators, the operators had a significant number of tasks to accomplish in responding to symptoms and specific events. The flow chart EOPs helped them by providing a symptom or parameter response "road-map" with all paths simultaneously visible. These paths are interrelated and operators are trained to afford them equal priority.
- The EOP's helped them focus their attention to the loss of control rod position indication, and directed their attention on reactor power, pressure and level.
- The operators reported that the EOPs and their related training gave them confidence in their actions.

8.7 Stabilizing Reactor Pressure

The EOPs did not provide sufficient guidance for stabilizing reactor vessel pressure.

- Operators are trained that the three flow paths for controlling reactor pressure, level, and power have equal priority and should be followed concurrently. Training also emphasizes the importance of maintaining core cooling by restoring and maintaining reactor vessel water level.
- During the event, operators were instructed by the EOPs to restore reactor vessel level using reactor core isolation cooling (RCIC). Following initiation of RCIC, the addition of cool water from the condensate storage tank, steam flow to the RCIC turbine and auxiliary steam loads caused reactor system pressure to decrease. RCIC flow was reduced by reactor operators when reactor vessel water level was restored to the desired normal level, while reactor pressure continued to decrease.
- The EOP pressure control path directs operators to continue to stabilize pressure until they determine that the reactor is shut down. No guidance is provided on how to prevent a pressure decrease either before or after the reactor is shut down. The reactor pressure path of the EOPs does not direct

nor prohibit the operators to manually close the main steam isolation valves to stabilize pressure for depressurization events.

- Operators had not received effective training in the control of water level and pressure simultaneously while using RCIC under the conditions posed by previous depressurization events.
- Rudimentary heat and mass balance calculations performed by the team using auxiliary steam loads supplied by the licensee could not explain the pressure decrease with which the operators had to cope during the event. An understanding of the reactor system pressure response is necessary to develop procedural guidance for RCIC operation following a reactor scram.

8.8 Scram Procedure Did Not Complement the Emergency Procedures

The scram procedure at NMP-2 did not complement the emergency operating procedures (EOPs) for ATWS conditions. This procedure does not support the operator by specifying priority actions (or immediate actions) to be used in conjunction with the EOPs for all scrams.

- The scram procedure at NMP-2 provides directions for actions to be taken after a normal scram.
- As discussed in Section 5.6.1, the directions in this procedure and the EOP reactor power path are incompatible for certain situations.
- The scram procedure direction to secure condensate booster pumps at the 202.3-inch level was located approximately half way through (i.e., the 23rd step) in this section of the procedure.
- The scram procedure does not distinguish immediate actions steps from supplemental action steps. Post-scram recovery actions are specified.
- The need for the above distinction is specified in the requirements for the applicable industry standard for this plant (ANSI/ANS-3.2 1982).

8.9 Lack of Recovery Procedures at Nine Mile Point Unit 2

Lack of certain recovery procedures unnecessarily challenged the operators during the event.

- Operators relied on experience-based knowledge to restore power to the loads normally powered from the lost UPS units. No procedure had been written for a loss of UPS as occurred in the August 13 event.
- Operators inappropriately closed feedwater pump suction valves in conformance with their procedures prior to restarting a condensate booster

pump. They were using the normal start-up procedure because there was no other available guidance.

8.10 Condensate Booster Pump Injections at Nine Mile Point Unit 2

Licensee actions in response to previous uncontrolled condensate booster pump injections were not effective in preventing their recurrence. Also, industry operating experience indicates that BWR-5-design reactors are more susceptible than other BWR designs to uncontrolled booster pump injections, and Nine Mile Point Unit 2 has had two previous events of this kind. BWR-6-design reactors have booster pump trips on high reactor vessel level, and the RCIC design in applicable older reactors results in condensate booster pump injections having less effect in reducing reactor pressure.

8.11 NRC Expectations on the Treatment of Balance of Plant Equipment

The NRC has not presented a clear position to the regulated industry concerning control of equipment configuration and treatment of important balance of plant equipment.

The UPS are important and within the scope of the NRC maintenance monitoring rule. However, the rule itself, had it been in effect, would not have changed the course of this event.

Much deliberation has occurred within the NRC and between the NRC and industry on the classification and treatment of important balance of plant equipment that is not classified as safety related, such as the UPS.

APPENDIX A

INCIDENT INVESTIGATION TEAM CHARTER

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

August 15, 1991

MEMORANDUM FOR: The Chairman
Commissioner Rogers
Commissioner Curtiss
Commissioner Remick

FROM: James M. Taylor
Executive Director
for Operations

SUBJECT: INVESTIGATION OF AUGUST 13, 1991 EVENT AT NINE MILE POINT,
UNIT 2 NUCLEAR POWER PLANT, INVOLVING REACTOR TRIP WITH LOSS
OF CONTROL ROOM ANNUNCIATORS AND PARTIAL LOSS OF PLANT
INSTRUMENTATION

On August 13, 1991 at 6:13 a.m. EDT, the licensee for the Nine Mile Point, Unit 2, Nuclear Power Plant notified the NRC that a Site Area Emergency had been declared for unit 2 due to a loss of annunciators and instrumentation with a plant transient. The loss of control room annunciators and partial loss of Balance of Plant instrumentation resulted from a loss of five uninterruptable power supplies when the phase B main transformer failed. At 6:22 a.m., power was restored to the annunciators and instrumentation and safe shut down conditions were verified. The plant scrambled early in the event, which began at 6:00 a.m. All safety systems remained available during this event, except for one train of low pressure coolant injection, which was out of service for maintenance. At 7:06 a.m. the plant commenced a normal cooldown using secondary systems.

An Augmented Inspection Team (AIT) was immediately sent to the site by Region I to investigate the event. However, because of the potential safety significance and the regulatory questions the event raises, I have requested AEOD to take the necessary actions to upgrade the current AIT to a seven member NRC Incident Investigation Team (IIT). Arrangements are being made under the provisions of a Memorandum of Agreement with the Institute of Nuclear Power Operations for industry participation. The team is to: (a) fact find as to what happened; (b) identify the probable cause as to why it happened; and (c) make appropriate findings and conclusions which would form the basis for any necessary follow-on actions.

The team will report directly to me and is comprised of: Jack Rosenthal (AEOD), Team Leader; Jose Ibarra (NRR); Michael Jordan (RIII); John Kauffman (AEOD); Frank Ashe (NRR); Walton Jensen (NRR) and Richard Conte (RI). Enclosed is the charter for the IIT to use in the review of the event.

The IIT was selected on the bases of their knowledge and experience in the fields of reactor systems, reactor operations, human factors and power distribution systems. Team members other than Mr. Conte have no direct involvement with Nine Mile Point. Mr. Conte will provide continuity from the AIT effort which began August 13, 1991. The additional team members and team leader are currently enroute to the site.

The licensee has agreed to preserve the equipment in accordance with a Confirmatory Action Letter which was issued by the Regional Administrator on August 13, 1991 and supplemented on August 15, 1991. The licensee has also agreed not to restart Nine Mile Point, Unit 2, until concurrence is received from the NRC.

The IIT report will constitute the single NRC fact-finding investigation report except for emergency preparedness and radiological consequences, which will be reviewed by Region I. It is expected that the team report will be issued within 45 days from now.

James M. Taylor
Executive Director
for Operations

Enclosure: As stated

cc: SECY
OGC
ACRS
GPA
Regional Administrators

ENCLOSURE

Incident Investigation Team Charter

Reactor Trip with Loss of Control Room Annunciators and
Partial Loss of Plant Instrumentation

The scope of the IIT investigation should be focused on a detailed review of the electrical system design, equipment response to the electrical disruption and the challenges the electrical system failures placed on operations personnel. The review will include conditions preceding the event, event chronology, safety significance, precursors to the event and whether the regulatory process and activities preceding the event contributed to it. Within the framework of this scope, the IIT should specifically:

With respect to conditions preceding the event: Identify the initial plant conditions (prior to the main transformer fault). Identify the internal and/or external conditions that led to the transformer fault.

With respect to the event chronology: Develop and validate a detailed sequence of events associated with the main transformer fault, loss of control room annunciation, partial loss of instrumentation, partial loss of emergency lighting and communications systems, reactor trip and reactor building equipment losses. Include in the event chronology the sequence of steps associated with the restoration of the required equipment.

With respect to plant system response: Evaluate the loss of control room annunciators and indications, balance of plant (BOP) instrumentation, emergency lighting and communication systems, and the loss of five uninterruptable power supplies (UPS) and establish an understanding of why certain other UPS continued to function.

With respect to human factors considerations: Assess the challenge to the operators and their ability to cope with it, including control room and equipment operator actions in response to the loss of control room annunciation and instrumentation, as well as emergency lighting and communication systems.

With respect to equipment performance: Evaluate the adequacy of the design, maintenance, separation and protective features of the UPS for the initial main transformer fault.

Region I will continue appropriate inspection efforts in review of emergency preparedness, radiological and other considerations. Issues identified by the IIT but outside the scope of this charter will be referred to Region I for inspection followup.

The scope of the investigation does not include:

Assessing violations of NRC rules and requirements; and reviewing the design and licensing bases for the facility, except as necessary to assess the cause for the event under investigation.

APPENDIX B

IE Bulletin No. 79-27, LOSS OF NON-CLASS 1E INSTRUMENTATION AND CONTROL POWER SYSTEM BUS DURING OPERATION

UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF INSPECTION AND ENFORCEMENT
WASHINGTON, D.C. 20555

SSINS No.: 6820
Accession No.:
7910250499

November 30, 1979

IE Bulletin No. 79-27

LOSS OF NON-CLASS-1-E INSTRUMENTATION AND CONTROL POWER SYSTEM BUS
DURING OPERATION

Description of Circumstances:

On November 10, 1979, an event occurred at the Oconee Power Station, Unit 3, that resulted in loss of power to a non-class-1-E 120 Vac single phase power panel that supplied power to the Integrated Control System (ICS) and the Non-Nuclear Instrumentation (NNI) System. This loss of power resulted in control system malfunctions and significant loss of information to the control room operator.

Specifically, at 3:16 p.m., with Unit 3 at 100 percent power, the main condensate pumps tripped, apparently as a result of a technician performing maintenance on the hotwell level control system. This led to reduced feedwater flow to the steam generators, which resulted in a reactor trip due to high coolant system pressure and simultaneous turbine trip at 3:16:57 p.m. At 3:17:15 p.m., the non-class-1-E inverter power supply feeding all power to the integrated control system (which provides proper coordination of the reactor, steam generator feedwater control, and turbine) and to one NNI channel tripped and failed to automatically transfer its loads from the DC power source to the regulated AC power source. The inverter tripped due to blown fuses. Loss of power to the NNI rendered control room indicators and recorders for the reactor coolant system (except for one wide-range RCS pressure recorder) and most of the secondary plant systems inoperable, causing loss of indication for systems used for decay heat removal and water addition to the reactor vessel and steam generators. Upon loss of power, all valves controlled by the ICS assumed their respective failure positions. The loss of power existed for approximately three minutes, until an operator could reach the equipment room and manually switch the inverter to the regulated AC source.

The above event was discussed in IE Information Notice No. 79-29, issued November 16, 1979.

NUREG 0600 "Investigation into the March 28, 1979 TMI Accident" also discusses TMI LER 78-021-03L whereby the RCS depressurized and Safety Injection occurred on loss of a vital bus due to inverter failure.

Actions to Be Taken by Licensees

For all power reactor facilities with an operating license and for those nearing completion of construction (North Anna 2, Diablo Canyon, McGuire, Salem 2, Sequoyah, and Zimmer):

1. Review the class-1-E and non-class 1-E buses supplying power to safety and non-safety related instrumentation and control systems which could affect the ability to achieve a cold shutdown condition using existing procedures or procedures developed under item 2 below. For each bus:
 - a) identify and review the alarm and/or indication provided in the control room to alert the operator to the loss of power to the bus.
 - b) identify the instrument and control system loads connected to the bus and evaluate the effects of loss of power to these loads including the ability to achieve a cold shutdown condition.
 - c) describe any proposed design modifications resulting from these reviews and evaluations, and your proposed schedule for implementing those modifications.
2. Prepare emergency procedures or review existing ones that will be used by control room operators, including procedures required to achieve a cold shutdown condition, upon loss of power to each class 1-E and non-class 1-E bus supplying power to safety and non-safety related instrument and control systems. The emergency procedures should include:
 - a) the diagnostics/alarms/indicators/symptom resulting from the review and evaluation conducted per item 1 above.
 - b) the use of alternate indication and/or control circuits which may be powered from other non-class 1-E or class 1-E instrumentation and control buses.
 - c) methods for restoring power to the bus.

Describe any proposed design modification or administrative controls to be implemented resulting from these procedures, and your proposed schedule for implementing the changes.
3. Re-review IE Circular No. 79-02, Failure of 120 Volt Vital AC Power Supplies, dated January 11, 1979, to include both class 1-E and non-class 1-E safety related power supply inverters. Based on a review of operating experience and your re-review of IE Circular No. 79-02, describe any proposed design modifications or administrative controls to be implemented as a result of the re-review.
4. Within 90 days of the date of this Bulletin, complete the review and evaluation required by this Bulletin and provide a written response describing your reviews and actions taken in response to each item.

Reports should be submitted to the Director of the appropriate NRC Regional Office and a copy should be forwarded to the NRC Office of Inspection and Enforcement, Division of Reactor Operations Inspection, Washington, D.C. 20555.

If you desire additional information regarding this matter, please contact the IE Regional Office.

Approved by GAO B180225 (R0072); clearance expires 7/31/80. Approval was given under a blanket clearance specifically for identified generic problems.

RECENTLY ISSUED
IE BULLETINS

Bulletin No.	Subject	Date Issued	Issued To
79-26	Boron Loss From BWR Control Blades	11/20/79	All BWR power reactor facilities with an OL
79-25	Failures of Westinghouse BFD Relays In Safety-Related Systems	11/2/79	All power reactor facilities with an OL or CP
79-17 (Rev. 1)	Pipe Cracks In Stagnant Borated Water System At PWR Plants	10/29/79	All PWR's with an OL and for information to other power reactors
79-24	Frozen Lines	9/27/79	All power reactor facilities which have either OLs or CPs and are in the late stage of construction
79-23	Potential Failure of Emergency Diesel Generator Field Exciter Transformer	9/12/79	All Power Reactor Facilities with an Operating License or a construction permit
79-14 (Supplement 2)	Seismic Analyses For As-Built Safety-Related Piping Systems	9/7/79	All Power Reactor Facilities with an OL or a CP
79-22	Possible Leakage of Tubes of Tritium Gas in Timepieces for Luminosity	9/5/79	To Each Licensee who Receives Tubes of Tritium Gas Used in Timepieces for Luminosity
79-13 (Rev. 1)	Cracking in Feedwater System Piping	8/30/79	All Designated Applicants for OLs
79-02 (Rev. 1) (Supplement 1)	Pipe Support Base Plate Designs Using Concrete Expansion Anchor Bolts	8/20/79	All power Reactor Facilities with an OL or a CP
79-14 (Supplement)	Seismic Analyses For As-Built Safety-Related Piping Systems	8/15/79	All Power Reactor Facilities with an OL or a CP

APPENDIX C

Generic Letter 83-28, REQUIRED ACTIONS BASED ON GENERIC IMPLICATIONS OF SALEM ATWS EVENT

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

July 8, 1983

TO ALL LICENSEES OF OPERATING REACTORS, APPLICANTS FOR OPERATING
LICENSE, AND HOLDERS OF CONSTRUCTION PERMITS

Gentlemen:

SUBJECT: REQUIRED ACTIONS BASED ON GENERIC IMPLICATIONS OF SALEM
ATWS EVENTS (Generic Letter 83-28)

The Commission has recently reviewed intermediate-term actions to be taken by licensees and applicants as a result of the Salem anticipated transient without scram (ATWS) events. These actions have been developed by the staff based on information contained in NUREG-1000, "Generic Implications of ATWS Events at the Salem Nuclear Power Plant." These actions address issues related to reactor trip system reliability and general management capability.

The actions covered by this letter fall into the following four areas:

1. Post-Trip Review - This action addresses the program, procedures and data collection capability to assure that the causes for unscheduled reactor shutdowns, as well as the response of safety-related equipment, are fully understood prior to plant restart.
2. Equipment Classification and Vendor Interface - This action addresses the programs for assuring that all components necessary for accomplishing required safety-related functions are properly identified in documents, procedures, and information handling systems that are used to control safety-related plant activities. In addition, this action addresses the establishment and maintenance of a program to ensure that vendor information for safety-related components is complete.
3. Post-Maintenance Testing - This action addresses post-maintenance operability testing of safety-related components.
4. Reactor Trip System Reliability Improvements - This action is aimed at assuring that vendor-recommended reactor trip breaker modifications and associated reactor protection system changes are completed in PWRs, that a comprehensive program of preventive maintenance and surveillance testing is implemented for the reactor trip breakers in PWRs, that the shunt trip attachment activates automatically in all PWRs that use circuit breakers in their reactor trip system, and to ensure that on-line functional testing of the reactor trip system is performed on all LWRs.

The enclosure to this letter breaks down these actions into several components. You will find that all actions, except four (Action 1.2, 4.1, 4.3, and 4.5), require software (procedures, training, etc.) changes and/or modifications and do not affect equipment changes or require reactor shutdown to complete. Action 1.2 may result in some changes to the sequence of events recorder or existing plant computers, but will not result in a plant shutdown to implement. Actions 4.1, 4.3 and 4.5.2, if applicable, would require the plant to be shutdown in order to implement.

The reactor trip system is fundamental to reactor safety for all nuclear power plant designs. All transient and accident analyses are predicated on its successful operation to assure acceptable consequences. Therefore, the actions listed below, which relate directly to the reactor trip system, are of the highest priority and should be integrated into existing plant schedules first.

- 1.1 Post-Trip Review (Program Description and Procedure)
- 2.1 Equipment Classification and Vendor Interface (Reactor Trip System Components)
- 3.1 Post-Maintenance Testing (Reactor Trip System Components)
- 4.1 Reactor Trip System Reliability (Vendor-Related Modifications)
- 4.2.1 and 4.2.2 Reactor Trip System Reliability (Preventive Maintenance and Surveillance Program for Reactor Trip Breakers)
- 4.3 Reactor Trip System Reliability (Automatic Actuation of Shunt-trip Attachment for Westinghouse and B&W plants)

Most of the remaining intermediate-term actions concern all other safety-related systems. These systems, while not sharing the same relative importance to safety as the reactor trip system, are essential in mitigating the consequences of transients and accidents. Therefore, these actions should be integrated into existing plant schedules over the longer-term on a medium priority basis. Some of the actions discussed in the enclosure will best be served by Owners' Group participation, and this is encouraged to the extent practical.

Accordingly, pursuant to 10 CFR 50.54(f), operating reactor licensees and applicants for an operating license (this letter is for information only for those utilities that have not applied for an operating license) are requested to furnish, under oath and affirmation, no later than 120 days from the date of this letter, the status of current conformance with the positions contained herein, and plans and schedules for any needed improvements for conformance with the positions. The schedule for the implementation of these improvements is to be negotiated with the Project Manager.

Licensees and applicants may request an extension of time for submittals of the required information. Such a request must set forth a proposed schedule and justification for the delay. Such a request shall be directed to the Director, Division of Licensing, NRR. Any such request must be submitted no later than 60 days from the date of this letter. If a licensee or applicant does not intend to implement any of the enclosed items, the response should so indicate and a safety basis should be provided for each item not intended to be implemented. Value-impact analysis can be used to support such responses or to argue in favor of alternative positions that licensees might propose.

For Operating Reactors, the schedules for implementation of these actions shall be developed consistent with the staff's goal of integrating new requirements, considering the unique status of each plant and the relative safety importance of the improvements, combined with all other existing plant programs. Therefore, schedules for implementation of these actions will be negotiated between the NRC Project Manager and licensees.

For plants undergoing operating license review at this time, plant-specific schedules for the implementation of these requirements shall be developed in a manner similar to that being used for operating reactors, taking into consideration the degree of completion of the power plant. For construction permit holders not under OL review and for construction permit applicants, the requirements of this letter shall be implemented prior to the issuance of an operating license.

This request for information was approved by the Office of Management and Budget under clearance number 3150-0011 which expires April 30, 1985. Comments on burden and duplication may be directed to the Office of Management and Budget, Reports Management Room 3208, New Executive Office Building, Washington, D. C. 20503.

Sincerely,

Darrell G. Eisenhut, Director
Division of Licensing

Enclosure:
Required Actions Based on Generic
Implications of Salem ATWS Events

ENCLOSURE

REQUIRED ACTIONS BASED ON GENERIC IMPLICATIONS OF SALEM ATWS EVENTS

1.1 POST-TRIP REVIEW (PROGRAM DESCRIPTION AND PROCEDURE)

Position

Licensees and applicants shall describe their program for ensuring that unscheduled reactor shutdowns are analyzed and that a determination is made that the plant can be restarted safely. A report describing the program for review and analysis of such unscheduled reactor shutdowns should include, as a minimum:

1. The criteria for determining the acceptability of restart.
2. The responsibilities and authorities of personnel who will perform the review and analysis of these events.
3. The necessary qualifications and training for the responsible personnel.
4. The sources of plant information necessary to conduct the review and analysis. The sources of information should include the measures and equipment that provide the necessary detail and type of information to reconstruct the event accurately and in sufficient detail for proper understanding. (See Action 1.2)
5. The methods and criteria for comparing the event information with known or expected plant behavior (e.g., that safety-related equipment operates as required by the Technical Specifications or other performance specifications related to the safety function).
6. The criteria for determining the need for independent assessment of an event (e.g., a case in which the cause of the event cannot be positively identified, a competent group such as the Plant Operations Review Committee, will be consulted prior to authorizing restart) and guidelines on the preservation of physical evidence (both hardware and software) to support independent analysis of the event.
7. Items 1 through 6 above are considered to be the basis for the establishment of a systematic method to assess unscheduled reactor shutdowns. The systematic safety assessment procedures compiled from the above items, which are to be used in conducting the evaluation, should be in the report.

Applicability

This position applies to all licensees and OL applicants.

Type of Review

For licensees, a post-implementation review of the program and procedures will be conducted or the staff will perform a pre-implementation review if desired by the licensee. NRR will perform the review and issue Safety Evaluations.

For OL applicants, the NRR review will be performed consistent with the licensing schedule.

Documentation Required

Licensees and applicants shall submit a report describing their program addressing all the items in the position.

Technical Specification Changes Required

No changes to Technical Specifications are required.

References

Section 2.2 of NUREG-1000
Regulatory Guide 1.33
ANSI N18.7-1976/ANS-3.2
Item I.C.5 of NUREG-0660
10 CFR 50 - 50.72

1.2 POST-TRIP REVIEW - DATA AND INFORMATION CAPABILITY

Position

Licensees and applicants shall have or have planned a capability to record, recall and display data and information to permit diagnosing the causes of unscheduled reactor shutdowns prior to restart and for ascertaining the proper functioning of safety-related equipment.

Adequate data and information shall be provided to correctly diagnose the cause of unscheduled reactor shutdowns and the proper functioning of safety-related equipment during these events using systematic safety assessment procedures (Action 1.1). The data and information shall be displayed in a form that permits ease of assimilation and analysis by persons trained in the use of systematic safety assessment procedures.

A report shall be prepared which describes and justifies the adequacy of equipment for diagnosing an unscheduled reactor shutdown. The report shall describe as a minimum:

1. Capability for assessing sequence of events (on-off indications)
 1. Brief description of equipment (e.g., plant computer, dedicated computer, strip chart)
 2. Parameters monitored
 3. Time discrimination between events
 4. Format for displaying data and information
 5. Capability for retention of data and information
 6. Power source(s) (e.g., Class IE, non-Class IE, non-interruptable)
2. Capability for assessing the time history of analog variables needed to determine the cause of unscheduled reactor shutdowns, and the functioning of safety-related equipment.
 1. Brief description of equipment (e.g., plant computer, dedicated computer, strip charts)
 2. Parameters monitored, sampling rate, and basis for selecting parameters and sampling rate
 3. Duration of time history (minutes before trip and minutes after trip)

4. Format for displaying data including scale (readability) of time histories
 5. Capability for retention of data, information, and physical evidence (both hardware and software)
 6. Power source(s) (e.g., Class IE, non-Class IE, non-interruptible)
3. Other data and information provided to assess the cause of unscheduled reactor shutdowns.
 4. Schedule for any planned changes to existing data and information capability.

Applicability

This position applies to all licensees and OL applicants.

Type of Review

Data and information capability will be reviewed by NRR to determine whether adequate data and information will be available to support the systematic safety assessment of unscheduled reactor shutdowns. NRR will perform the reviews and issue a Safety Evaluation.

For licensees, a post-implementation review of the program and procedures will be conducted by NRR or the staff will perform a pre-implementation review if desired by the licensee.

For OL applicants, the NRR review will be performed consistent with the licensing schedule.

Documentation Required

Licensees and applicants shall submit a report describing their data and information capability for unscheduled reactor shutdowns.

Technical Specification Changes Required

To be determined based on evaluation of required documentation.

References

Section 2.2 of NUREG-1000.

2.1 EQUIPMENT CLASSIFICATION AND VENDOR INTERFACE (REACTOR TRIP SYSTEM COMPONENTS)

Position

Licensees and applicants shall confirm that all components whose functioning is required to trip the reactor are identified as safety-related on documents, procedures, and information handling systems used in the plant to control safety-related activities, including maintenance, work orders, and parts replacement. In addition, for these components, licensees and applicants shall establish, implement and maintain a continuing program to ensure that vendor information is complete, current and controlled throughout the life of the plant, and appropriately referenced or incorporated in plant instructions and procedures. Vendors of these components should be contacted and an interface established. Where vendors can not be identified, have gone out of business, or will not supply the information, the licensee or applicant shall assure that sufficient attention is paid to equipment maintenance, replacement, and repair, to compensate for the lack of vendor backup, to assure reactor trip system reliability. The vendor interface program shall include periodic communication with vendors to assure that all applicable information has been received. The program should use a system of positive feedback with vendors for mailings containing technical information. This could be accomplished by licensee acknowledgement for receipt of technical mailings. The program shall also define the interface and division of responsibilities among the licensees and the nuclear and nonnuclear divisions of their vendors that provide service on reactor trip system components to assure that requisite control of and applicable instructions for maintenance work are provided.

Applicability

This action applies to all licensees and OL applicants.

Type of Review

For licensees, a post-implementation review will be conducted. NRR will perform these licensing reviews and issue a Safety Evaluation.

For OL applicants, the NRR review will be performed consistent with the licensing schedule.

Documentation Required

Licensees and applicants should submit a statement confirming that they have reviewed the Reactor Trip System components and conform to the position regarding equipment classification. In addition, a summary report describing the vendor interface program shall be submitted for staff review. Vendor lists of technical information, and the technical information itself, shall be available for inspection at each reactor site.

Technical Specification Changes Required

No changes to Technical Specifications are required.

Reference

Section 2.3.1 of NUREG-1000.

Section 2.3.2 of NUREG-1000.

2.2 EQUIPMENT CLASSIFICATION AND VENDOR INTERFACE (PROGRAMS FOR ALL SAFETY-RELATED COMPONENTS)

Position

Licensees and applicants shall submit, for staff review, a description of their programs for safety-related* equipment classification and vendor interface as described below:

1. For equipment classification, licensees and applicants shall describe their program for ensuring that all components of safety-related systems necessary for accomplishing required safety functions are identified as safety-related on documents, procedures, and information handling systems used in the plant to control safety-related activities, including maintenance, work orders and replacement parts. This description shall include:
 1. The criteria for identifying components as safety-related within systems currently classified as safety-related. This shall not be interpreted to require changes in safety classification at the systems level.
 2. A description of the information handling system used to identify safety-related components (e.g., computerized equipment list) and the methods used for its development and validation.
 3. A description of the process by which station personnel use this information handling system to determine that an activity is safety-related and what procedures for maintenance, surveillance, parts replacement and other activities defined in the introduction to 10 CFR 50, Appendix B, apply to safety-related components.
 4. A description of the management controls utilized to verify that the procedures for preparation, validation and routine utilization of the information handling system have been followed.
 5. A demonstration that appropriate design verification and qualification testing is specified for procurement of safety-related components. The specifications shall include qualification testing for expected safety service conditions and provide support for the licensees' receipt of testing documentation to support the limits of life recommended by the supplier.

*Safety-related structures, systems, and components are those that are relied upon to remain functional during and following design basis events to ensure: (1) the integrity of the reactor coolant boundary, (2) the capability to shut down the reactor and maintain it in a safe shutdown condition, and (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the guidelines of 10 CFR Part 100.

6. Licensees and applicants need only to submit for staff review the equipment classification program for safety-related components. Although not required to be submitted for staff review, your equipment classification program should also include the broader class of structures, systems, and components important to safety required by GDC-1 (defined in 10 CFR Part 50, Appendix A, "General Design Criteria, Introduction").
2. For vendor interface, licensees and applicants shall establish, implement and maintain a continuing program to ensure that vendor information for safety-related components is complete, current and controlled throughout the life of their plants, and appropriately referenced or incorporated in plant instructions and procedures. Vendors of safety-related equipment should be contacted and an interface established. Where vendors cannot be identified, have gone out of business, or will not supply information, the licensee or applicant shall assure that sufficient attention is paid to equipment maintenance, replacement, and repair, to compensate for the lack of vendor backup, to assure reliability commensurate with its safety function (GDC-1). The program shall be closely coupled with action 2.2.1 above (equipment qualification). The program shall include periodic communication with vendors to assure that all applicable information has been received. The program should use a system of positive feedback with vendors for mailings containing technical information. This could be accomplished by licensee acknowledgment for receipt of technical mailings. It shall also define the interface and division of responsibilities among the licensee and the nuclear and nonnuclear divisions of their vendors that provide service on safety-related equipment to assure that requisite control of and applicable instructions for maintenance work on safety-related equipment are provided.

Applicability

This action applies to all licensees and OL applicants.

Type of Review

For licensees, a post-implementation review will be conducted. NRR will perform the review and issue a Safety Evaluation.

For OL applicants, the NRR review will be performed consistent with the licensing schedule.

Documentation Required

Licensees and applicants should submit a report that describes the equipment classification and vendor interface programs outlined the position above.

Technical Specification Changes Required

No changes to the Technical Specifications are required.

References

Section 2.3.1 of NUREG-1000.

Section 2.3.2 of NUREG-1000.

3.1 POST-MAINTENANCE TESTING (REACTOR TRIP SYSTEM COMPONENTS)

Position

The following actions are applicable to post-maintenance testing:

1. Licensees and applicants shall submit the results of their review of test and maintenance procedures and Technical Specifications to assure that post-maintenance operability testing of safety-related components in the reactor trip system is required to be conducted and that the testing demonstrates that the equipment is capable of performing its safety functions before being returned to service.
2. Licensees and applicants shall submit the results of their check of vendor and engineering recommendations to ensure that any appropriate test guidance is included in the test and maintenance procedures or the Technical Specifications, where required.
3. Licensees and applicants shall identify, if applicable, any post-maintenance test requirements in existing Technical Specifications which can be demonstrated to degrade rather than enhance safety. Appropriate changes to these test requirements, with supporting justification, shall be submitted for staff approval. (Note that action 4.5 discusses on-line system functional testing.)

Applicability

This action applies to all licensees and OL applicants.

Type of Review

For licensees, a post-implementation review will be conducted for actions 3.1.1 and 3.1.2 above. The Regions will perform these licensing reviews and issue Safety Evaluations. Proposed Technical Specification changes resulting from action 3.1.3 above will receive a pre-implementation review by NRR.

For OL applicants, the review will be performed consistent with the licensing schedule.

Documentation Required

Licensees and applicants should submit a statement confirming that actions 3.1.1 and 3.1.2 of the above position have been implemented.

Technical Specification Changes Required

Changes to Technical Specifications, as a result of action 3.1.3, are to be determined by the licensee or applicant and submitted for staff approval, as necessary.

Reference

Section 2.3.4 of NUREG-1000.

3.2 POST-MAINTENANCE TESTING (ALL OTHER SAFETY-RELATED COMPONENTS)

Position

The following actions are applicable to post-maintenance testing:

1. Licensees and applicants shall submit a report documenting the extending of test and maintenance procedures and Technical Specifications review to assure that post-maintenance operability testing of all safety-related equipment is required to be conducted and that the testing demonstrates that the equipment is capable of performing its safety functions before being returned to service.
2. Licensees and applicants shall submit the results of their check of vendor and engineering recommendations to ensure that any appropriate test guidance is included in the test and maintenance procedures or the Technical Specifications where required.
3. Licensees and applicants shall identify, if applicable, any post-maintenance test requirements in existing Technical Specifications which are perceived to degrade rather than enhance safety. Appropriate changes to these test requirements, with supporting justification, shall be submitted for staff approval.

Applicability

This action applies to all licensees and OL applicants.

Type of Review

For licensees, a post-implementation review will be conducted for actions 3.2.1 and 3.2.2 above. The Regions will perform these licensing reviews and issue Safety Evaluations. Proposed Technical Specification changes resulting from action 3.2.3 above will receive a pre-implementation review by NRR.

For OL applicants, the review will be performed consistent with the licensing schedule.

Documentation Required

Licensees and applicants should submit a statement confirming that actions 3.2.1 and 3.2.2 of the above position have been implemented.

Technical Specification Changes Required

Changes to Technical Specifications, as a result of action 3.2.3, are to be determined by the licensee or applicant for staff approval, as necessary.

Reference

4.1 REACTOR TRIP SYSTEM RELIABILITY (VENDOR-RELATED MODIFICATIONS)

Position

All vendor-recommended reactor trip breaker modifications shall be reviewed to verify that either: (1) each modification has, in fact, been implemented; or (2) a written evaluation of the technical reasons for not implementing a modification exists.

For example, the modifications recommended by Westinghouse in NCD-Elec-18 for the DB-50 breakers and a March 31, 1983, letter for the DS-416 breakers shall be implemented or a justification for not implementing shall be made available. Modifications not previously made shall be incorporated or a written evaluation shall be provided.

Applicability

This action applies to all PWR licensees and OL applicants.

Type of Review

For licensees, a post-implementation review will be conducted. The Regions will perform these licensing reviews and issue Safety Evaluations.

For OL applicants, the NRR review will be performed consistent with the licensing schedule.

Documentation Required

Licensees and applicants should submit a statement confirming that this action has been implemented.

Technical Specifications Required

No changes to Technical Specifications are required.

Reference

Section 3 of NUREG-1000.

4.2 REACTOR TRIP SYSTEM RELIABILITY (PREVENTATIVE MAINTENANCE AND SURVEILLANCE PROGRAM FOR REACTOR TRIP BREAKERS)

Position

Licensees and applicants shall describe their preventative maintenance and surveillance program to ensure reliable reactor trip breaker operation. The program shall include the following:

1. A planned program of periodic maintenance, including lubrication, housekeeping, and other items recommended by the equipment supplier.
2. Trending of parameters affecting operation and measured during testing to forecast degradation of operability.
3. Life testing of the breakers (including the trip attachments) on an acceptable sample size.
4. Periodic replacement of breakers or components consistent with demonstrated life cycles.

Applicability

This action applies to all PWR licensees and OL applicants.

Type of Review

Actions 4.2.1 and 4.2.2 will receive a post-implementation review by NRR. A pre-implementation review will be performed by NRR for actions 4.2.3 and 4.2.4 (the circuit breaker life testing program and the component testing/replacement requirements based upon the life testing results). A Safety Evaluation will be issued.

For OL applicants, NRR will perform the reviews for actions 4.2.1 and 4.2.2 on a schedule consistent with the licensing schedule. NRR will perform a pre-implementation review for actions 4.2.3 and 4.2.4 (the circuit breaker life testing program and the component testing/replacement requirements based upon the life testing results). Safety Evaluations will be issued.

Documentation Required

Licensees and applicants should submit descriptions of their programs to ensure compliance with this action.

Technical Specification Changes Required

No changes to Technical Specifications are required.

Reference

Section 3 of NUREG-1000.

4.3 REACTOR TRIP SYSTEM RELIABILITY (AUTOMATIC ACTUATION OF SHUNT TRIP ATTACHMENT FOR WESTINGHOUSE AND B&W PLANTS)

Position

Westinghouse and B&W reactors shall be modified by providing automatic reactor trip system actuation of the breaker shunt trip attachments. The shunt trip attachment shall be considered safety related (Class IE).

Applicability

This action applies to all Westinghouse and B&W licensees and OL applicants.

Type of Review

For licensees, a pre-implementation review shall be performed for the design modifications by NRR. A Safety Evaluation will be issued.

For OL applicants, the NRR review will be performed consistent with the licensing schedule.

Technical Specification changes, if required, will be reviewed prior to implementation.

Documentation Required

Licensees and applicants should submit a report describing the modifications.

Technical Specification Changes Required

Licensees are to submit any needed Technical Specification change requests prior to declaring the modified system operable.

Reference

Section 3 of NUREG-1000.

4.4 REACTOR TRIP SYSTEM RELIABILITY (IMPROVEMENTS IN MAINTENANCE AND TEST PROCEDURES FOR B&W PLANTS)

Position

Licensees and applicants with B&W reactors shall apply safety-related maintenance and test procedures to the diverse reactor trip feature provided by interrupting power to control rods through the silicon controlled rectifiers.

This action shall not be interpreted to require hardware changes or additional environmental or seismic qualification of these components.

Applicability

This action applies to B&W licensees and OL applicants only.

Type of Review

For licensees, a post-implementation review will be conducted. The Regions will conduct the licensing review and issue a Safety Evaluation.

For OL applicants, the review will be performed consistent with the licensing schedule.

Documentation Required

Licensees and applicants should submit a statement confirming that this action has been implemented.

Technical Specification Changes Required

Include the silicon controlled rectifiers in the appropriate surveillance and test sections of the Technical Specifications.

Reference

Section 3 of NUREG-1000.

4.5 REACTOR TRIP SYSTEM RELIABILITY (SYSTEM FUNCTIONAL TESTING)

Position

On-line functional testing of the reactor trip system, including independent testing of the diverse trip features, shall be performed on all plants.

1. The diverse trip features to be tested include the breaker undervoltage and shunt trip features on Westinghouse, B&W (see Action 4.3 above) and CE plants; the circuitry used for power interruption with the silicon controlled rectifiers on B&W plants (see Action 4.4 above); and the scram pilot valve and backup scram valves (including all initiating circuitry) on GE plants.
2. Plants not currently designed to permit periodic on-line testing shall justify not making modifications to permit such testing. Alternatives to on-line testing proposed by licensees will be considered where special circumstances exist and where the objective of high reliability can be met in another way.
3. Existing intervals for on-line functional testing required by Technical Specifications shall be reviewed to determine that the intervals are consistent with achieving high reactor trip system availability when accounting for considerations such as:
 1. uncertainties in component failure rates
 2. uncertainty in common mode failure rates
 3. reduced redundancy during testing
 4. operator errors during testing
 5. component "wear-out" caused by the testing

Licensees currently not performing periodic on-line testing shall determine appropriate test intervals as described above. Changes to existing required intervals for on-line testing as well as the intervals to be determined by licensees currently not performing on-line testing shall be justified by information on the sensitivity of reactor trip system availability to parameters such as the test intervals, component failure rates, and common mode failure rates.

Applicability

This action applies to all licensees and OL applicants.

Type of Review

For licensees, a post-implementation review will be conducted for action 4.5.1. The Regions will perform these licensing reviews and issue Safety Evaluations. Actions 4.5.2 and 4.5.3 will require a pre-implementation review by NRR. Results will be issued in a Safety Evaluation.

For OL applicants, the NRR review should be performed consistent with the licensing schedule.

Documentation Required

For item 4.5.1, licensees and applicants should submit a statement confirming that this action has been implemented.

For item 4.5.2, licensees and applicants should submit a report describing the modifications for staff review.

For item 4.5.3, licensees and applicants should submit proposed Technical Specification changes for staff review.

Technical Specification Changes Required

For licensees, Technical Specification changes are required.

For OL applicants, Technical Specifications will be incorporated as part of the license.

Reference

Section 3 of NUREG-1000.

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

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

NUREG-1455

3. DATE REPORT PUBLISHED

MONTH

YEAR

OCTOBER

1991

4. FIN OR GRANT NUMBER

2. TITLE AND SUBTITLE

TRANSFORMER FAILURE AND COMMON-MODE LOSS OF
INSTRUMENT POWER AT NINE MILE POINT UNIT 2
ON AUGUST 13, 1991

5. AUTHOR(S)

INCIDENT INVESTIGATION TEAM

6. TYPE OF REPORT

INVESTIGATIVE

7. PERIOD COVERED (Inclusive Dates)

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

OFFICE OF THE EXECUTIVE DIRECTOR FOR OPERATIONS
U.S. NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555

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.)

OFFICE OF THE EXECUTIVE DIRECTOR FOR OPERATIONS
U.S. NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

On August 13, 1991, at Nine Mile Point Unit 2 nuclear power plant, located near Scriba, New York, on Lake Ontario, the main transformer experienced an internal failure that resulted in degraded voltage which caused the simultaneous loss of five uninterruptible power supplies, which in turn caused the loss of several nonsafety systems, including reactor control rod position indication, some reactor power and water indication, control room annunciators, the plant communications system, the plant process computer, and lighting at some locations. The reactor was subsequently brought to a safe shutdown. Following this event, the U.S. Nuclear Regulatory Commission dispatched an Incident Investigation Team to the site to determine what happened, to identify the probable causes, and to make appropriate findings and conclusions. This report describes the incident, the methodology used by the team in its investigation, and presents the teams findings and conclusions.

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

Civilian Nuclear Power
Incident Investigation
Transformer Fault
Loss of Instrumentation

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

(This Page)

Unclassified

(This Report)

Unclassified

15. NUMBER OF PAGES

16. PRICE

END

**DATE
FILMED**

12/05/91