WCAP-14114
Rev 0

Human Performance in Operating Events: Lessons Learned for the AP600 M-MIS Design

Emilie M. Roth
Westinghouse Science & Technology Center

Table of Contents

1.0 Introduction 1
1.1 Background 3
2.0 Cases where M-MIS resources failed to support detection/observation 7
2.1 Cases where the plant parameter indicators required for monitoring or control were unavailable or inadequate 7
2.2 Cases where operators failed to detect an abnormal (but not alarmed) condition 8
3.0 Cases where M-MIS resources failed to support situation assessment 9
3.1 Cases where there were misleading indicators (failed sensors). 9
Implications for AP600 MMI
3.2 Cases where operators had to determine whether a plant indicator was spurious. 10
4.0 Cases where the M-MIS Resources failed to support response planning 12
4.1 Cases where the particular situation was not fully covered by the procedure requiring knowledge-based reasoning to fill in gaps and adapt to the situation. 12
4.2 Cases where operators had to balance multiple goals in determining course of action 14
4.3 Cases where operators bypassed safety features. 16
4.4 Cases that raise a concern that the delay entailed in performing EOP E-0 may negatively impact recovery ability. 17
4.5 Cases where procedures were available but not used 18
5.0 Cases where operator actions reflected gaps in knowledge (implying a need for improved training) 20
6.0 Cases where workload was high or workload distribution across crew members was ineffectual 23
6.1 Cases where there were low levels of task awareness, command, control and communication 23
6.2 Cases where operators failed to take a required action due to a mental lapse. 25
6.3 Cases where high administrative workload reduced the ability of operator crews to respond to the emergency. 26
7.0 References 28
Appendix 29

1.0 Introduction

This report summarizes some lessons learned with respect to requirements for improved human performance in nuclear power plant (NPP) emergencies based on review of selected recent reports examining operator performance in emergency incidents in nuclear power plants. The reports reviewed are:

Kauffman, J. V., G. F. Lanik, E. A. Trager, and R. A. Spence, *Operating Experience Feedback Report – Human Performance in Operating Events*, NUREG-1275, Office for Analysis and Evaluation of Operational Data, U.S. Nuclear Regulatory Commission, Washington, D.C. December, 1992.

NRC, NUREG-1455, *Transformer Failure and Common-Mode Loss of Instrument Power at Nine Mile Point Unit 2 on August 13, 1991*. U.S. Nuclear Regulatory Commission, Washington, DC 20555, October, 1991.

NRC, NRC Augmented Inspection Team Exit Meeting Presentation for Salem Unit 1 Reactor Trip with Multiple Safety Injections, handout, April 26, 1994.

Wreathall, J., Reason, J. and Dougherty, Jr. E. M. "Latent Failures and Human Performance in Significant Operating Events", draft report prepared for Division of Systems Research Office of Nuclear Regulatory Research U.S. Nuclear Regulatory Commission, July, 1993.

Collectively these reports include analyses of 23 recent NPP emergency incidents. These incidents were examined for evidence of problems in the man-machine interface system (M-MIS), training, or procedures that contributed to human performance problems. Based on review of these reports a number of cases were identified where the M-MIS, procedures and/or training, failed to adequately support operator cognitive activity during the emergencies. A classification scheme was developed that classifies events based on the type of operator cognitive activity that was <u>not</u> adequately supported. The classes identified were:

- Cases where M-MIS resources failed to support detection/observation
  - Cases where the plant parameter indicators required for monitoring or control were unavailable or inadequate
  - Cases where operators failed to detect an abnormal (but not alarmed) condition
- Cases where M-MIS resources failed to support situation assessment
  - Cases where there were misleading indicators (failed sensors)
- Cases where operators had to determine whether a plant indicator was spurious

- Cases where the M-MIS Resources failed to support response planning
  - Cases where the particular situation was not fully covered by the procedure requiring knowledge-based reasoning to fill in gaps and adapt to the situation
  - Cases where operators had to balance multiple goals in determining course of action
  - Cases where operators bypassed safety features
  - Cases that raise a concern that the delay entailed in performing EOP E-0 may negatively impact recovery ability
  - Cases where procedures were available but not used
- Cases where operator actions reflected gaps in knowledge (implying a need for improved training)
- Cases where workload was high or workload distribution across crew members was ineffectual
  - Cases where there were low levels of task awareness, command, control and communication
  - Cases where operators failed to take a required action due to a mental lapse
  - Cases where high administrative workload reduced the ability of operator crews to respond to the emergency

Sections 2 – 6 of this report are organized around the classes of the classification scheme. For each class, summaries are provided of NPP emergency incidents where that type of situation arose. This is followed by a discussion of the implications for design of the AP-600 M-MIS. This includes discussion of how planned AP-600 M-MIS resources are expected to reduce the potential for the types of human performance problems identified.

Section 1.1 provides background on the two main reports that were used as sources of incident descriptions: a report by the Office for Analysis and Evaluation of Operational Data (AEOD) of the U.S. Nuclear Regulatory Commission published in 1992 (NUREG-1275), and a follow-up report produced by the Division of Systems Research of the Office of Nuclear Regulatory Research that is currently in draft form (Wreathall, Reason & Dougherty, 1993). Section 1.1 summarizes the main results and conclusions of these reports. The analysis presented in Sections 2 – 6 are consistent with, and extend the conclusions of these two reports.

1.1 Background

In 1992 the AEOD published a report summarizing the results of a study examining human performance during 16 power reactor events that occurred between 1990 and 1992 (NUREG-1275). The purpose of the AEOD study was to identify the factors that contributed to good operator performance during the events, as well as the factors that hindered performance, and feed this information back to the industry. The AEOD report identified a number of weaknesses in control room organization, procedures, and human machine interface.

The main conclusions of the AEOD report were:

1. *Control Room Organization.* The AEOD report concluded that in some cases control room staffing levels and other organizational weaknesses impaired crews in performing their emergency functions. In particular the AEOD report suggested that the practice of utilizing a "dual-role" senior technical advisor (STA), where one of the Senior Reactor Operators (SRO) takes on the responsibility of the STA during emergencies had drawbacks. At plants that employed a "dual-role" STA control room management personnel were overburdened during emergencies. In some cases the AOED judged that tasks, supervision, and technical oversight were not appropriately allocated. The AEOD report concluded that difficulties due to control room organization and task assignments could be minimized, in most cases without additional staff, by changes to control room shift structure and assignments based on functional analysis (including STA functions) and lessons learned from analysis of operating events.

2. *Procedures.* The AEOD report concluded that procedure problems were key contributors in the less successful events. One problem noted was *procedure adherence*. Some operators acted during events without using a procedure. The AEOD report concluded that procedure content, ease of use, and management policy and practices influenced procedure use.

3. *Need for "knowledge-based reasoning."* The AEOD report indicated that in some cases operators experienced difficulty in applying knowledge to unusual plant conditions during events, which resulted in delays in recognizing and responding to events. The report concluded that some knowledge-based performance is necessary in every event to recognize the significance of the situation, initiate use of the appropriate abnormal operating procedures or EOPs, and follow those procedures to respond to events. While procedures are available for a large number of potential accidents and transients, some situations will arise where existing procedures do not apply. Thus, knowledge-based performance will be necessary at times, to return the plant to a safe condition.

4. *Human-Machine Interface.* The AEOD report concluded that a lack of appropriately ranged, direct-reading, control room instrumentation to monitor reactor pressure, temperature, and level caused operators to have difficulty in recognizing and responding to shutdown events, when operator actions were required to accomplish the safety functions of disabled, automatic safety systems. The AEOD report also concluded that annunciator and computer alarms were important operator aids in recognizing and responding to events. In fact, operators failed to recognize conditions that were clearly off-normal, but which were not alarmed.

Subsequent to the AEOD report the Office of Nuclear Regulatory Research of the U.S. NRC had J. Wreathall, J. Reason, and E. Dougherty expand the analysis of human performance in NPP incidents (Wreathall, Reason & Dougherty, Jr., draft, 1993). They expanded the analysis to include a total of 21 events, and employed a human error analysis framework to identify the influences that appeared to distinguish events that involved more successful and less successful human performance. The results they obtained were consistent with the results of the AEOD report.

Wreathall et al. (1993) divided the 21 events they examined into 10 "more successful" and 11 "less successful" events. They then examined the events in each class for the presence of deficiencies in procedures, training, organization, and human-machine interaction (HMI). Two analyses were performed. In one analysis they used a 2-point rating scheme: deficiency present or absent. In the second analysis they used a 3-point rating scheme: 0 = deficiency not noted as a factor, 1 = deficiency of minor significance and 2 = deficiency of major significance. Figures 1 and 2 summarize the results of these analyses respectively.

Procedures was found to be a major contributor to problems in performance. Of the 11 "less successful" events 100% were judged to have a procedure problem. When a 3-point rating scheme was used the total score for "less successful" events was 82% of the maximum possible total score. For the 10 more successful events 60% of the time there was a procedure problem. When a 3-point rating scheme was used the total score for "more successful" events was still 35%. Note that the reduced percentage of observed procedure problems for "successful" events does not necessarily mean that procedure problems did not exist in those events. It is possible that procedure problems were not detected in those cases because operators were knowledgeable and were able to compensate for procedure limitations.

In the case of training, organization, and HMI problems, the percentage of events with deficiencies observed were 59%, 86% and 41% for the less successful events, and 10%, 10% and 25% for the more successful events.

The main conclusions to be drawn from the AEOD report and the follow-up report by Wreathall et al. is that procedures, training, and M-MIS continue to be problematic. The high proportion of events, both successful and unsuccessful, where deficiencies in procedures were observed, make clear that situations that are not fully addressed by procedures often arise and

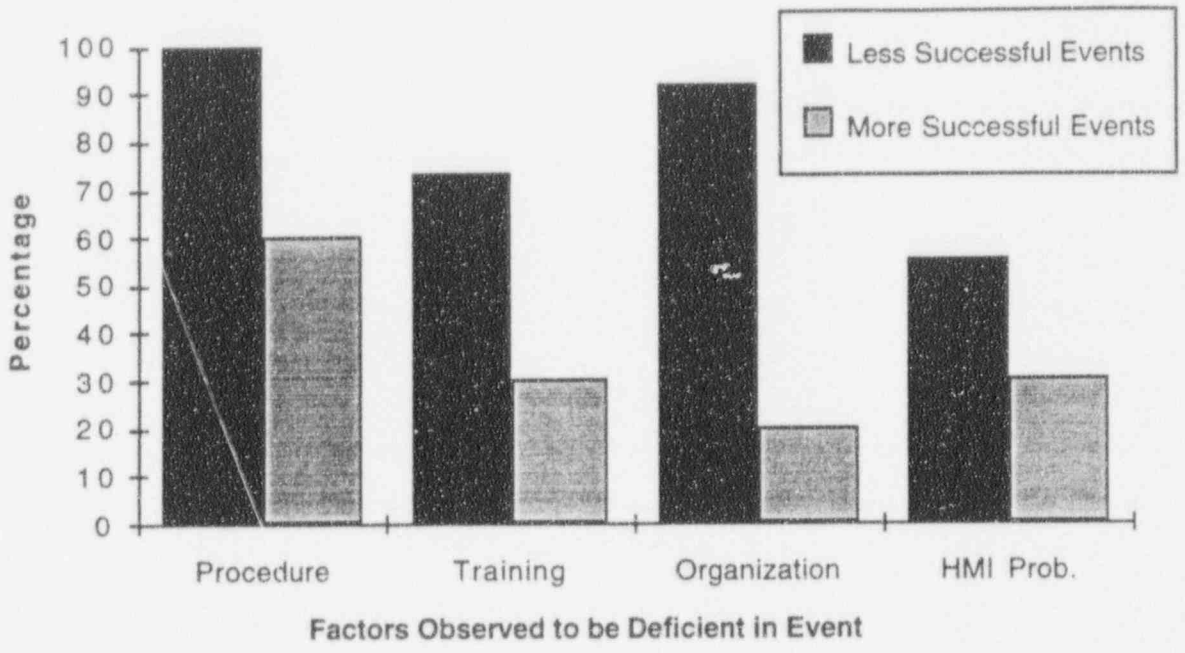

Figure 1. Percentage of 11 'less successful' and 10 'more successful' events where deficiencies in procedures, training, organization, and HMI were observed (adapted from Wreathall, et al., 1993).

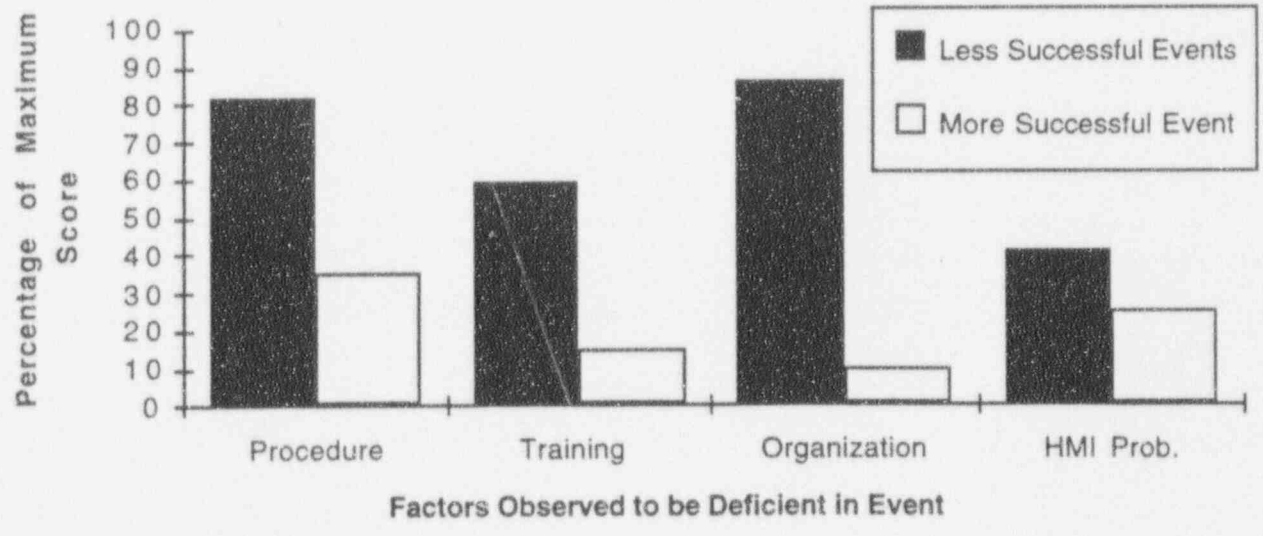

Figure 2. Percentage of maximum total score (using a 3-point scale) obtained for the 11 'less successful' and 10 'more successful' events (adapted from Wreathall, et al., 1993).

that it is important to provide operators with resources and training to support the type of knowledge-based reasoning that is required in those situations (cf., Roth, Mumaw, and Lewis, in press.)

These results affirm the validity of the AP-600 M-MIS design philosophy of providing M-MIS resources to support operator cognitive activity such as situation assessment and response planning, and the importance of providing operator training in these cognitive activities.

In Sections 2 – 6 a more detailed classification is provided of the types of cases that arose in the 23 incidents examined that revealed deficiencies in supporting operator cognitive activity. In each case we discuss the implications for design of AP-600 M-MIS resources to more effectively support operator cognitive activity.[1]

---

[1] More detailed analyses of the cognitive factors that contributed to crew performance problems in two events, Mine Mile Point Unit 2 and Crystal River Unit 3, are provided in the Appendix.

2.0 Cases Where M-MIS Resources Failed to Support Detection/ Observation

2.1 Cases where the plant parameter indicators required for monitoring or control were unavailable or inadequate.

- *Peach Bottom Unit 3 – Loss of Electrohydraulic Fluid (1/28/90)*

  The plant was at 99.8 percent power. A leak of electrohydraulic control fluid occurred from a main turbine control valve. Power was reduced and a manual trip was performed. The leak was stopped and reactor level was stabilized.

  Because of the lack of a direct-reading flow instrument, control of high-pressure coolant injection (HPCI) flow to the reactor vessel was erratic.

- *Prairie Island Unit 2 – Loss of Shutdown Cooling (2/20/92)*

  The event occurred during a refueling outage while a reactor vessel draining to midloop was in progress. A loss of shutdown cooling resulted from insufficient water level in the RCS.

  A tygon tube was the only instrument providing usable RCS level information during the draindown. Operators had difficulty reading the level correctly in the tygon tube due to parallax problems, poor lighting and tube visibility degraded by the tube penetrating the next floor. To obtain actual level tygon tube levels were transformed via manual calculation to correct for the nitrogen pressure effects. Round off errors during water level calculations contributed to inaccurate estimates of RCS level.

- *Catawba Unit 1 – Reactor Coolant System Overpressurization (3/20/90)*

  The plant was in cold shutdown. The operators were performing reactor fill and vent operations. During initial pressurization of the reactor coolant system the operators overpressurized the reactor coolant system and the residual heat removal system because they were monitoring pressure instrumentation that was inoperable.

  Even if the instrumentation had been operating the operators needed to determine reactor pressure that was near zero psig. The instrumentation available ranged from 0 to 3000 psig, and 0 to 800 psig. Small pressure changes of the type expected during fill and vent operations would not be noticeable on these instruments.

Implications for AP600 MMI:

Function-based task analyses that systematically identify instrumentation requirements to support monitoring and control during all modes of operation will minimize the potential for inadequate instrumentation.

2.2 Cases where operators failed to detect an abnormal (but not alarmed) condition

- *Quad Cities Unit 2 – Main Steam Isolation (9/18/91)*

  The reactor was in an end-of-cycle coastdown and the main steam line B isolated causing power to spike from 83% to 98%. The control room crew did not identify this power spike until three hours later.

  No alarms came on because no set points were exceeded.

  The Unit 2 nuclear station operator who was responsible for monitoring the panels overlooked the indicated loss of flow in main steam line B, the momentary spike in level and power, and the sustained elevation in reactor pressure.

  The control room organization failed to catch this oversight until the offnormal condition was identified by chance during a surveillance by another nuclear station operator.

Implications for AP600 MMI:

The AWARE system employs advanced technology to manage alarms. This will increase the probability that high priority alarms are detected

The failure to detect an abnormal condition can be avoided by using a smarter alarm management system such as AWARE that changes alarm set points based on power level considerations.

The wall panel information system will support monitoring key plant parameters by multiple crew members.

3.0 Cases where M-MIS resources failed to support situation assessment

3.1 Cases where there were misleading indicators (failed sensors).

- ***Catawba Unit 1 – Reactor Coolant System Overpressurization (3/20/90)***

  The operators overpressurized the RCS and the RHR system because they were monitoring RCS pressure instrumentation that was inoperable.

  The operators were not aware that all three RCS pressure instrument transmitters were still isolated following welding of the tube fittings during the refueling outage. RCS pressure rose faster than anticipated (in 2.5 hours vs. 4-6 hours in previous similar pressurizations). Operators did not observe RHR discharge pressure indicator. Operators recognized a potential problem when the PRT level began to rise and searched for the leakage path from the RCS. The high RHR system pressure was noticed by a systems engineer who entered the control room at around that point.

  There were other parameters the operators could have used to cross-check RCS pressure values. Pressure changes in the chemical and volume control system and RHR systems could have been used to confirm changes in RCS pressure.

- ***Crystal River Unit 3 – Pressurizer Spray Valve Failure (12/08/91)***

  At about 10 percent power, a slow loss of RCS pressure was observed. The actuator for the pressurizer spray line control valve had failed open, however, the valve continued to indicate closed.

  The operators did not realize why the RCS pressure was decreasing until the pressurizer spray line isolation valve was closed about an hour later. (The pressurizer spray line isolation valve was closed at the recommendation of a manager with SRO qualifications who was senior to the shift supervisor).

- ***Prairie Island Unit 2 – Loss of Shutdown Cooling (2/20/92)***

  The event occurred during a refueling outage while a reactor vessel draining to midloop was in progress. A loss of shutdown cooling resulted from insufficient water level in the RCS.

  When the draindown started, the electronic level instrument display on the control room emergency response computer system was off-scale high.

Implications for AP600 MMI:

Displays, training, and procedures will encourage monitoring of multiple converging indicators to confirm situation assessment.

Another possibility to consider is "smart" displays that do some automatic cross-checking in computing data quality. The plant computer could be used to perform instrument cross-checks to alert operators to defective instruments.

3.2 Cases where operators had to determine whether a plant indicator was spurious.

- *LaSalle County Unit 2 – Reactor Water Cleanup System Isolation Bypass. (4/20/92)*

While at 20% power the Nuclear Station Operator shut down the Reactor Water Cleanup (RWCU) System, as part of the test procedures for verifying the limit switch settings. The actions he took were in the reverse order to that stated in the procedure substeps, resulting in a high-differential flow alarm, indicating the start of a 45-second delay timer preceding the automatic RWCU isolation.

The operators bypassed the automatic RWCU isolation for three minutes while they worked as a team to verify that the alarm was not spurious. An equipment attendant identified flow through a RWCU regenerative heat exchanger relief valve. A third Nuclear Station Operator found reactor building equipment drain tank level increasing, while the 95 gpm RWCU differential flow continued. This allowed them to establish that the RWCU alarm was not spurious.

- ***Oconee Unit 3 – Loss of Shutdown Cooling (3/08/91)***

The event occurred during a refueling outage. Technicians performing a test opened an emergency sump suction valve creating a drain pat from the hot leg. The water level in the reactor vessel fell to the bottom of the hot leg causing a loss of shutdown cooling until the valve was reclosed.

The operators questioned the validity of the reactor vessel level reading and verified it by high containment sump level and low hot leg level.

- ***Fort Calhoun – Stuck Open Relief Valve (7/03/92)***

A partial loss of electric load led to over pressurization of the reactor coolant system sufficient to lift the two power-operated relief valves as well as one safety relief valve (lifting of the safety relief valve may not have been anticipated in the design basis). The safety relief valve did not reclose leading to a LOCA. The safety systems designed to mitigate the LOCA (i.e., safety injection) worked, and the operators shut down the plant successfully.

A twenty-degree subcooling margin is required to optimize the cooldown of the reactor post-LOCA and to throttle safety injection. The Emergency Response Facility Computer System displayed subcooling but included a flag that indicated questionable data for subcooling margin. As a result operators ignored that reading and relied instead on an RCS pressure indicator on the control board that provided inaccurate readings (there was a lag in pressure indication). The operators did not compute subcooling but relied rather on observation that pressure tracked temperature. On this basis the operators decided to throttle safety injection in accordance with the procedures. Subsequent analysis showed that subcooling margin was lost and voiding occurred as a result of the throttling of SI by the operators.

The throttling of safety injection was interpreted as an error of commission (Wreathall, Reason, & Dougherty, 1993).

Implications for AP600 MMI:

Displays, training, and procedures will encourage monitoring of multiple converging indicators to confirm situation assessment.

Another possibility to consider is "smart" displays that do some automatic cross-checking in computing data quality.

4.0 Cases where the M-MIS Resources failed to support response planning

4.1 Cases where the particular situation was not fully covered by the procedure requiring knowledge-based reasoning to fill in gaps and adapt to the situation.

- ***Peach Bottom Unit 3 – Loss of Electrohydraulic Fluid (1/28/90)***

  The plant was at 99.8 percent power. A leak of electrohydraulic control fluid occurred from a main turbine control valve. Power was reduced and a manual trip was performed. The leak was eventually stopped and reactor level was stabilized.

  Operators attempted to establish reactor feed flow from condensate pump A – but failed because they did not close the suction valves for reactor feedwater pumps A and B. The procedure they were using for reactor feed with condensate pump A was written for plant startup when the feedwater pump suction valves were normally closed.

- ***Nine Mile Point Unit 2 – Partial Loss of Instrument Air (5/14/90)***

  A partial loss of instrument air occurred.

  The "Instrument and Service Air System Procedure" was written primarily to address a total loss of instrument air rather than partial losses of the system.

- ***Nine Mile Point Unit 2 – Transformer Failure and Common-Mode Loss of Instrument Power (August 13, 1991)***

  The Nine Mile Point incident involved a loss of uninterruptible power sources that resulted in extensive loss of control room plant indicators. One outcome was that while automatic reactor protection systems, including the scram, functioned properly, control rod position indication was lost so operators could not definitively exclude the possibility of a failure of scram. As a result they took the conservative action in accordance with their procedures, of responding as if there had been no scram.

  Operators experienced difficulty restarting the feedwater pumps because the startup procedures did not address quick restart of feedwater and condensate pumps under emergency conditions.

- ***Dresden Unit 2 – Stuck Open Safety Relief Valve (8/02/90)***

  A safety relief valve failed open resulting in a plant trip.

Although spurious opening of a safety relief valve is an anticipated event for a boiling water reactor, there was no event-specific guidance for plant cooldown in the plant procedures or training materials.

- ***Quad Cities Unit 2 – Reactor Scram Due to Control Rod Withdrawal (10/17/90)***

  The plant was in hot standby. The reactor scrammed on hi-hi intermediate range flux because the operator withdrew rods to increase reactor pressure without recognizing the need to follow the normal procedures for reestablishing reactor criticality.

  The procedure had no special instructions for reactivity management and no cautions about possible high rod notch worths.

- ***Millstone Unit 3 – Turbine Building Pipe Rupture (12/31/90)***

  The plant was at 86% power. Two 6 inch diameter moisture separator condensate return drain lines ruptured and discharged hot condensate system steam and water to the turbine building.

  The control room operators manually initiated a reactor trip and a main steam line isolation and began recovery activities.

  Following the trip, the operators found that they had lost automatic control of pressurizer level. The operators and instrument and control technicians deduced that moisture in the turbine building caused a loss of power that isolated instrument air to the letdown valves and pressurizer spray valves. They devised a method to restore instrument air to containment and thus restore normal control of RCS inventory and pressure.

- ***Monticello – Hi-Hi IRM Scram (6/06/91)***

  Operators terminated a reactor startup and began a reactor shutdown to repair a leaking safety relief valve. The method used to shut down the reactor was notch insertion of control rods. Because the decay heat rate was less than steam loads, the reactor cooled and positive reactivity was added to the core. The RO did not compensate for this cooldown. Reactor power increased and resulted in the reactor scram.

  The shutdown procedure did not contain cautions or notes regarding the positive reactivity when the steam load was greater than the decay heat rate or options to counter a significant cooldown. This event occurred when a normal startup was terminated and transition was made to the shutdown procedure. Because the startup was terminated at an early stage,

the crew had to determine where they were in the shutdown process and which steps in the procedure were applicable.

- ***Prairie Island Unit 2 – Loss of Shutdown Cooling (2/20/92)***

  The event occurred during a refueling outage while a reactor vessel draining to midloop was in progress. A loss of shutdown cooling resulted from insufficient water level in the RCS.

  Operators entered the abnormal procedure for "Loss of Coolant While in a Reduced Inventory Condition." Operators observed from the rate of level increase and heatup that actions of the abnormal procedure were insufficient to mitigate the transient before reaching entry conditions of the emergency procedures. RCS temperature was about 133 deg. F at the time of the running RHR pump trip. One entry condition for EOP "Core Cooling Following Loss of RHR Flow," required RCS temperature to be at 190 deg. F. The emergency procedure was immediately implemented when the temperature reached 190 deg. F.

Implications for AP600 MMI:

The MMI will support operator performance in situations that require adaptation of procedures to the particulars of the event. In these situations operators rely on "knowledge-based" reasoning.

The workstation functional and physical displays and AWARE system will support operator situation assessment and response planning in these cases.

Training, procedures, and control room MMI will reinforce each other in insuring that operators formulate an accurate situation assessment, identify appropriate goals, monitor procedure effectiveness in achieving these goals, recognize when procedures are not adequate to handle the situation and take action to fill in gaps in the procedure and adapt the procedure to the situation as necessary.

4.2 Cases where operators had to balance multiple goals in determining course of action

- ***Nine Mile Point Unit 2 – Transformer Failure and Common-Mode Loss of Instrument Power (August 13, 1991)***

  The Nine Mile Point incident involved a loss of uninterruptible power sources that resulted in extensive loss of control room plant indicators. One outcome was that while automatic reactor protection systems, including the scram, functioned properly, control rod position indication was lost so operators could not definitively exclude the possibility of a

failure of scram. As a result they took the conservative action in accordance with their procedures, of responding as if there had been no scram.

Among the human performance problems identified by the investigation team was that the operators took control actions intended to bring Reactor Vessel Water Level back up to normal, allowing Reactor Vessel Pressure to significantly drop. This illustrates a case where operators needed to balance conflicting goals (maintaining level and pressure). The Boiling Water Reactor flowchart procedures leave wide discretion to the operators with respect to prioritization among goals; while operators knew that reactor vessel level should be stabilized, there was neither procedural guidance, nor clear cues as to what pressure targets to achieve or avoid. Operators had considerable evidence suggesting that the rods were in fact in and so they likely did not believe they were in an ATWS situation. If they were not in an ATWS then pressure decrease was less serious a problem. In addition operator training emphasized the need to maintain Reactor Vessel Level. There was less training on the potential effect of a pressure decrease on the risk of reactor recriticality.

- ***Crystal River Unit 3 – Pressurizer Spray Valve Failure (12/08/91)***

  Operators secured the high pressure injection system injection flow before the reactor coolant system pressure had risen well above the 1500 psig minimum for the subcooling margin requirements.

  Contributors included a perceived need by the operators to balance multiple safety goals. High pressure injection flow was stopped because of the operators' concerns about overfilling the pressurizer and lifting the safety valve or power operated relief valve.

Implications for AP600 MMI:

Situations arise where operators need to consider and balance multiple goals. MMI resources and training will support this activity.

Workstation functional displays are specifically designed to facilitate identification and balancing of multiple goals.

Operator training will also address this issue.

4.3 Cases where operators bypassed safety features.

- ***Crystal River Unit 3 – Pressurizer Spray Valve Failure (12/08/91)***

At about 10 percent power, a slow loss of RCS pressure was observed. The actuator for the pressurizer spray line control valve had failed open, however, the valve continued to indicate closed. The operators did not realize why the RCS pressure was decreasing until the pressurizer spray line isolation (block) valve was closed about an hour later.

The operating crew bypassed automatic engineered safety features (high pressure injection, emergency feedwater, emergency diesel generators, and partial containment isolation) actuation for about 6 minutes. This initial bypass of the ESF, while the plant pressure decrease was not understood, was not directed by abnormal or emergency procedures, and was not directed by shift supervision. (The shift supervisors were unaware that an engineered safety feature was bypassed. The fact that the ESF was bypassed was noticed by a manager with SRO qualifications who recommended that it be unbypassed.)

The normal bypassing of safety injection during plant shutdown at Crystal River Unit 3 may have conditioned the operators to respond as they had previously, instead of recognizing that the existing situation was different.

- ***LaSalle County Unit 2 – Reactor Water Cleanup System Isolation Bypass (4/20/92)***

While at 20% power the Nuclear Station Operator shut down the Reactor Water Cleanup (RWCU) System, as part of the test procedures for verifying the limit switch settings. The actions he took were in the reverse order to that stated in the procedure substeps, resulting in a high-differential flow alarm, indicating the start of a 45-second delay timer preceding the RWCU isolation.

The NSO wanted to preserve the test and obtained the shift foreman's permission to bypass the automatic RWCU isolation (an engineered safety feature).

About 3 minutes later, the operators worked as a team to verify that the alarm was not spurious and decided to unbypass the RWCU automatic isolation.

A key element in this event was that several weeks earlier, an RWCU isolation had occurred because of a spurious RWCU high-differential flow signal resulting in damage to the RWCU containment isolation valve motors. The operators had been criticized for allowing the spurious isolation.

Implications for AP600 MMI:

Operators bypassing safety systems is a serious problem. One of the factors contributing to bypassing of safety systems is the fact that operators are placed in goal conflict situations. Efforts should be made to reduce the potential for goal conflict situations in the design of hardware systems as well as in the plant management and organizational climate.

The AP600 passive safety system design will reduce the potential for operators bypassing safety systems.

4.4 Cases that raise a concern that the delay entailed in performing EOP E-0 may negatively impact recovery ability.

- *Fort Calhoun – Stuck Open Relief Valve (7/03/92)*

A partial loss of electric load led to over pressurization of the reactor coolant system sufficient to lift the two power-operated relief valves as well as one safety relief valve (lifting of the safety relief valve may not have been anticipated in the design basis). The safety relief valve did not reclose leading to a LOCA. The safety systems designed to mitigate the LOCA (i.e., safety injection) worked, and the operators shut down the plant successfully.

In this event there was a ten minute elapsed time in implementing E-0. According to Dougherty (Wreathall, Reason and Dougherty, 1993) while the ten minute duration did not interfere with subsequent mitigation activities in this event it is not a time lag that can be ignored in all scenarios.

There is some suggestion that delays in performing E-0 activities may have contributed to complications that arose in the Salem Unit 1 Reactor Trip With Multiple Safety Injections Event (April 7, 1984). According to the NRC Augmented Inspection Team Exit Meeting presentation materials operator action extended the time to meet the emergency core cooling injection termination criteria in the emergency operating procedures. As a result the pressurizer filled up, producing a "solid" RCS.

Implications for AP600 MMI:

The inherent fixed linearity of paper-based procedures means that in some cases operators are placed in the situation where they have to go through procedure steps that are obviously not relevant to the situation and as a consequence delay reaching procedure steps that are important to perform in an expeditious manner. The Salem Unit 1 incident, where the pressurizer overfilled before the operators were able to reach the step in the procedure directing them to throttle safety injection, may be a case in point.

The inherent fixed linearity of paper-based procedures has two potential negative consequences. First, in some cases the delays caused by the need to follow each procedure step sequentially will result in conditions becoming more degraded than if operators could reach the relevant procedures steps more quickly. Second, because operators are able to assess the situation more quickly than the procedures allow, and in their experience they are generally correct, the temptation to jump to what they perceive to be the relevant steps for terminating the incident is high. This is likely to be a contributing factor in cases where operators are observed to "wing it" without procedures.

Properly designed, the computerized procedures for the AP600 plant will reduce these problems by enabling crews to reach relevant procedure steps more quickly.

4.5 Cases where procedures were available but not used

- ***LaSalle County Unit 2 – Reactor Water Cleanup System Isolation Bypass (4/20/92)***

  While at 20% power the Nuclear Station Operator shut down the Reactor Water Cleanup (RWCU) System, as part of the test procedures for verifying the limit switch settings. The actions he took were in the reverse order to that stated in the procedure substeps, resulting in a high-differential flow alarm, indicating the start of a 45-second delay timer preceding the automatic RWCU isolation.

  The RO stated in an interview that he normally relied on memory and experience to handle emergencies, then used procedures afterward to check his actions, because of frequent procedure revisions and having to go through three pages to find the one step needed.

- ***Crystal River Unit 3 – Pressurizer Spray Valve Failure (12/08/91)***

  At about 10 percent power, a slow loss of RCS pressure was observed. The actuator for the pressurizer spray line control valve had failed open, however, the valve continued to indicate closed.

  The annunciator response procedure for low RCS pressure was not used by the operators. Hence, the investigation of the reactor depressurization was not systematic. Operators withdrew control rods to raise reactor power, temperature, and pressure even though actual Tave was stable and not the cause of the pressure decrease.

Implications for AP600 MMI:

Failure of operators to utilize procedures is a serious problem. The COMPRO computerized procedure system will encourage procedure use.

5.0 Cases where operator actions reflected gaps in knowledge (implying a need for improved training)

- *Dresden Unit 2 – Stuck Open Safety Relief Valve (8/02/90)*

  The Shift Engineer became concerned about the unexpected high rate of heatup of the suppression pool and without procedural guidance ordered opening two turbine bypass valves to reduce system pressure. The Shift Engineer believed it was necessary to reduce heat input tot the torus and hoped the safety relief valve would reseat. According to the AEOD report (NUREG-1275, vol. 8) this was a misjudgment that reflected "excessive concern with torus heatup and lack of concern for a high cooldown rate."

  At Dresden, simulator training scenarios typically used a stuck open relief valve as the initiating event for an anticipated transient without scram (ATWS). In those scenarios, the torus heats rapidly and the torus temperature is a concern of major significance. Operators stated that they had not been trained for the simpler event to its expected conclusions. The lack of training for expected simple events failed to highlight the fact that the concerns and response to worst-case scenarios are often different from those of simple events. This preconditioning may explain why the crew had unnecessary, unwarranted concern for torus temperature response in this event.

- *Quad Cities Unit 2 – Reactor Scram Due to Control Rod Withdrawal (10/17/90)*

  The plant was in hot standby. The reactor scrammed on hi-hi intermediate range flux because the operator withdrew rods to increase reactor pressure without recognizing the need to follow the normal procedures for reestablishing reactor criticality.

  The operator had difficulty integrating reactor theory and plant response. He withdrew control rods to raise pressure and received an automatic reactor scram when power increased rapidly while intermediate range monitors were not maintained on scale.

  Requalification training had not covered reactor operations in hot standby, and the operators had no special training or briefing for the special test.

- *Millstone Unit 3 – Turbine Building Pipe Rupture (12/31/90)*

  The plant was at 86% power. Two 6 inch diameter moisture separator condensate return drain lines ruptured and discharged hot condensate system steam and water to the turbine building.

A number of Unit 3 operations, maintenance, engineering, and other plant personnel had observed the steam leak before the pipe rupture. There was apparently a lack of awareness by these individuals that the through-wall pipe leak could be a precursor to a catastrophic failure.

- ***Monticello – Hi-Hi Intermediate Range Monitor Scram (6/06/91)***

  Operators terminated a reactor startup and began a reactor shutdown to repair a leaking safety relief valve. The method used to shut down the reactor was notch insertion of control rods. Because the decay heat rate was less than steam loads, the reactor cooled and positive reactivity was added to the core. The RO did not compensate for this cooldown. Reactor power increased and resulted in the reactor scram.

  The operating crew did not recognize that the steam loads combined with a low decay heat rate would cause a cooldown resulting in increased reactivity. In addition, the crew did not react to the alarms and indications of the cooldown or the reactor power increase.

  The crew did not anticipate the expected plant cooldown when shutting down the reactor under conditions of low decay heat and auxiliary steam loads. The RO did not understand the intermediate range monitor response to the power increase due to RCS cooldown when rod insertion was stopped.

  Procedures and training did not specifically address a shutdown with low decay heat levels.

- ***Prairie Island Unit 2 – Loss of Shutdown Cooling (2/20/92)***

  The event occurred during a refueling outage while a reactor vessel draining to midloop was in progress. A loss of shutdown cooling resulted from insufficient water level in the RCS.

  Procedures and training did not provide sufficient direction in nitrogen pressure control. The draindown ROs lacked awareness of how nitrogen pressures affected the draining process. The significance of round-off errors during water level calculations was not recognized by the ROs and had not bee addressed during training. As a result, incorrect information was used for the draindown.

- ***LaSalle County Unit 2 – Reactor Water Cleanup System Isolation Bypass (4/20/92)***

  While at 20% power the Nuclear Station Operator shut down the Reactor Water Cleanup (RWCU) System, as part of the test procedures for verifying the limit switch settings. The actions he took were in the reverse order to that stated in

the procedure substeps, resulting in a high-differential flow alarm, indicating the start of a 45-second delay timer preceding the RWCU isolation.

The operator shut down the RWCU by closing the system return valve before stopping the RWCU pumps, which was in reverse order to that in the procedure substep. The operator lacked understanding of the required order of performance of procedural directions.

- ***Crystal River Unit 3 – Pressurizer Spray Valve Failure (12/08/91)***

  At about 10 percent power, a slow loss of RCS pressure was observed. The actuator for the pressurizer spray line control valve had failed open, however, the valve continued to indicate closed.

  The operators did not realize why the RCS pressure was decreasing. An operator withdrew control rods in an attempt to raise power, and hence, Tave, thinking they were in a cooldown situation. In fact, the reactor depressurization was not due to a cooldown which should have been evident from the stable Tave.

Implications for AP600 MMI:

Many events required operators to form a situation assessment and determine appropriate actions based on their understanding of plant configuration, dynamics, and underlying physics. The events above demonstrate that in many cases the operators did not have sufficient knowledge of plant dynamics to form a correct situation assessment and identify appropriate action. This was particularly true during low power and shutdown operations.

Performance on these events substantiates the need for greater attention to be given to development of required operator knowledge and cognitive skill during training.

6.0 Cases where workload was high or workload distribution across crew members was ineffectual

6.1 Cases where there were low levels of task awareness, command, control and communication

- *Braidwood Unit 1 – Loss of Reactor Coolant (10/04/90)*

  The plant was in cold shutdown. Two surveillance procedures were being performed in parallel. A technical staff engineer stationed in the control room instructed a technical staff engineer in the auxiliary building to close a vent valve. Four minutes later without receiving confirmation that the vent valve had been closed, he instructed the auxiliary nuclear station operator to open a different valve as part of a different surveillance. This caused the RCS to be aligned to the inlet of the still open vent valve and resulted in hot reactor coolant spraying personnel in the auxiliary building.

  The AEOD report (NUREG-1275, vol. 8) concluded that command, control, and communication were not effective during the execution of these two surveillances. The Shift Control Room Engineer, the Shift Engineer, and the Unit Nuclear Station Operator were not sufficiently in command to offer oversight of the technical staff engineers activities nor be aware of changes in the RCS configuration. The technical staff engineers were performing a relatively complex, dynamic task while in a state of fatigue and there were no redundancies in place to help prevent errors.

- *Quad Cities Unit 2 – Reactor Scram Due to Control Rod Withdrawal (10/17/90)*

  The plant was in hot standby. It was the third shift. The reactor scrammed on hi-hi intermediate range flux because the operator withdrew rods to increase reactor pressure without recognizing the need to follow the normal procedures for reestablishing reactor criticality.

  The SROs did not adequately monitor control rod manipulations by the unit nuclear station operator.

  Information on similar events at other stations had not been disseminated to the ROs.

  The unit nuclear station operator did not report back any information to the Shift Control Room Engineer while executing the Shift Control Room Engineer's command to insert control rods, although the changes in rod positions and reactor power level were significant enough to justify supervisory overview by the Shift Control Room Engineer.

The communications between the shift engineer and the shift control room engineer and between the shift control room engineer and the nuclear station operator were minimal and did not contain cautions or directions to report information back.

Although shift 1 observed high-notch worth (and verbally reported it to shift 2), this was not recorded nor passed on to shift 3.

- ***Millstone Unit 3 – Turbine Building Pipe Rupture (12/31/90)***

  Two 6 inch diameter moisture separator condensate return drain lines ruptured and discharged hot condensate system steam and water to the turbine building.

  Station administrative procedures did not cover actions to be taken for through-wall pipe leaks in the system and did not caution personnel that these could be a precursor to a catastrophic failure.

  Command and control at the plant was diminished when the senior control operator elected to personally isolate the leaking pipe section in the turbine building.

- ***Prairie Island Unit 2 – Loss of Shutdown Cooling (2/20/92)***

  The event occurred during a refueling outage while a reactor vessel draining to midloop was in progress. A loss of shutdown cooling resulted from insufficient water level in the RCS.

  There was uncertainty as to who had responsibility and authority to make the decision to hold or stop draindown activity. The shift supervision assumed the ROs did not require continual supervision. An apparent hesitation by the draindown crew to communicate some concerns to the supervisors may have resulted from the ROs not working with their normal crew.

Implications for AP600 MMI:

These events illustrate failures to maintain broad awareness of ongoing activities and their implications. Of particular concern are failures of supervisory personnel in maintaining awareness of the activities of personnel under their direction.

The wall panel information system is intended to support broad situation awareness of plant state and operator activities. It will enhance the ability of operators to keep track of each others activities and catch errors.

Additional MMI resources as well as better definition of crew structure and roles will be considered to reduce the workload of supervisory personnel and enhance their ability to maintain broad situation awareness and supervisory control.

6.2 Cases where operators failed to take a required action due to a mental lapse.

- *Nine Mile Point Unit 2 – Transformer Failure and Common-Mode Loss of Instrument Power (August 13, 1991)*

  This incident involved a loss of uninterruptible power sources that resulted in extensive loss of control room plant indicators. One outcome was that while automatic reactor protection systems, including the scram, functioned properly, control rod position indication was lost so operators could not definitively exclude the possibility of a failure of scram. As a result they took the conservative action in accordance with their procedures, of responding as if there had been no scram. While the conclusion of the investigation team was that there were no serious errors in performance, among operator performance deficiencies with potential risk consequences that were identified by the team was the failure of operators to secure the condensate booster pumps. As a result when reactor vessel pressure decreased below the discharge pressure of the condensate booster pumps the pumps began to rapidly inject water causing reactor water level to rapidly increase.

  Operators failed to anticipate the need to secure the condensate booster pumps prior to reaching the condensate booster pump set point. This was likely due to a memory lapse. Contributors include: high mental workload and lack of explicit reminder cues that the condensate booster pumps would come on if not secured (e.g., cues could have been provided in procedures or, as part of advanced control room "significant message" displays that display messages reminding operators of automatic systems that are about to come on).

Implications for AP600 MMI:

This event illustrates that in high workload situations operators may fail to anticipate automated system actuation that may have negative consequences.

Significance message displays that provide indication of approaching automatic system set points are specifically designed to alert operators of upcoming events that they need to be concerned about.

6.3 Cases where high administrative workload reduced the ability of operator crews to respond to the emergency.

- *Dresden Unit 2 – Stuck Open Safety Relief Valve (8/02/90)*

  A safety relief valve failed open resulting in a plant trip.

  The control room emergency organization provided little assistance to the Shift Engineer. This plant had a "dual-role" shift technical advisor. During emergencies the Shift Control Room Engineer assumed the role of STA and the Shift Engineer directed control room operations. When the Shift Engineer became the emergency director and assumed command of control room activities, he had little assistance in analyzing the condition of the plant and in monitoring and evaluating operator activities. The Shift Control Room Engineer was making telephone notifications and the two shift foremen were out in the plant.

  Potential problems included (1) the Shift Engineer may have been less familiar with the current condition of the plant than the Shift Control Room Engineer who he relieved, (2) the Shift Control Room Engineer may have been too involved with the details of the operation to provide an objective overview of the situation to provide fresh eyes, and (3) the STA made state and local telephone notifications.

- *Nine Mile Point Unit 2 – Transformer Failure and Common-Mode Loss of Instrument Power (August 13, 1991)*

  The Nine Mile Point incident involved a loss of uninterruptible power sources that resulted in extensive loss of control room plant indicators. One outcome was that while automatic reactor protection systems, including the scram, functioned properly, control rod position indication was lost so operators could not definitively exclude the possibility of a failure of scram. As a result they took the conservative action in accordance with their procedures, of responding as if there had been no scram.

  The incident investigation team indicated that the shift supervisor serving as the emergency director during an event, encountered with "overload" while fulfilling duties involving EOP reading, event classification, fire protection concerns, and implementation of the emergency plan.

Implications for AP600 MMI:

The AEOD report (NUREG-1275) raises concern that current practices regarding crew role assignments during emergencies may result in overloading of the supervisory personnel.

The AEOD report argues that control room staffing levels and other organizational weaknesses impaired some crews in performing their emergency functions. At these plants control room management personnel were overburdened during emergencies when tasks, supervision, and technical oversight were not appropriately allocated.

The AEOD report particularly questions the practice of having a "dual-role" shift technical advisor. At some plants (e.g., Commonwealth Edison plants, including Dresden) the STA function is assumed by the Shift Control Room Engineer, who normally directs control room operations. The control room supervisory function is transferred to the Shift Engineer who directs and verifies the actions of the control room operators and serves as the emergency director. The report argues that the use of the "dual-role" STA impaired crew performance because the other SRO(s) were overloaded when one SRO assumed the STA role. Assignment of other tasks during events sometimes detracted from the STA's safety function. In some cases the STA spent much of his time on telephone notifications resulting in limited redundancy and independence in control room decision-making and limited checking of important control room activities. In contrast the AEOD report argues that in instances where there was a dedicated STA (e.g., Fort Calhoun) control room organization was more effective. On this basis the AEOD report suggests a positive value for a dedicated STA and a dedicated emergency communicator.

The AEOD report argues that difficulties due to control room organization and task assignments can be minimized without additional staff, by making changes to control room shift structure and assignments based on functional analysis (including STA functions) and lessons learned from analysis of operating events.

In the AP600 plant design more attention will be paid to defining the set of responsibilities and activities to be performed during emergencies, and identifying a task allocation structure that does not result in excessive workload for any crew member. This may be an activity that can be performed with the aid of input from the utilities.

7.0 References

Kauffman, J. V., G. F. Lanik, E. A. Trager, and R. A. Spence, *Operating Experience Feedback Report – Human Performance in Operating Events*, NUREG-1275, Office for Analysis and Evaluation of Operational Data, U.S. Nuclear Regulatory Commission, Washington, D.C., December, 1992.

NRC, NUREG-1455, *Transformer Failure and Common-Mode Loss of Instrument Power at Nine Mile Point Unit 2 on August 13, 1991*. U.S. Nuclear Regulatory Commission, Washington, D.C. 20555. October, 1991.

NRC, NRC Augmented Inspection Team Exit Meeting Presentation for Salem Unit 1 Reactor Trip with Multiple Safety Injections, handout, April 26, 1994.

Roth, E. M., Mumaw, R. J., & Lewis, P. M. An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies. Washington D.C.: U.S. Nuclear Regulatory Commission, in press. (NUREG/CR-6208)

Wreathall, J., Reason, J. and Dougherty, Jr. E. M. "Latent Failures and Human Performance in Significant Operating Events", draft report prepared for Division of Systems Research Office of Nuclear Regulatory Research U.S. Nuclear Regulatory Commission, July, 1993.

Appendix:
Analyses of Factors Contributing to Crew Performance Problems in Two Actual Events that were Cognitively Challenging

Nine Mile Point Unit 2 (described in NUREG-1455)

The Nine Mile Point incident involved a loss of uninterruptible power sources that resulted in extensive loss of control room plant indicators. One outcome was that while automatic reactor protection systems, including the scram, functioned properly, control rod position indication was lost so operators could not definitively exclude the possibility of a failure of scram. As a result they took the conservative action in accordance with their procedures, of responding as if there had been no scram. While the conclusion of the investigation team was that there were no serious errors in performance, two operator actions (or lack there of) were identified by the team as performance deficiencies that had potential risk consequences: 1) The operators took control actions intended to bring Reactor Vessel Water Level back up to normal, allowing Reactor Vessel Pressure to significantly drop; 2) The operators failed to secure the condensate booster pumps.

Brief analysis of the cognitive demands inherent in the situation suggests that contributors included:

a) *Need for operators to balance conflicting goals (maintaining level and pressure):* BWR flowchart procedures leave wide discretion to the operators with respect to prioritization among goals; while operators knew that reactor vessel level should be stabilized, there was neither procedural guidance, nor clear cues as to what pressure targets to achieve or avoid.

b) *Operator situation assessment and expectations:* Operators had considerable evidence suggesting that the rods were in fact in and so they likely did not believe they were in an ATWS situation. If they were not in an ATWS then pressure decrease was less serious a problem.

c) *Lack of operator knowledge:* According to NUREG-1455 operator training emphasized the need to maintain Reactor Vessel Level. There was less training on the potential effect of a pressure decrease on the risk of reactor recriticality.

d) *Mental Lapse:* Operators failed to secure the condensate booster pumps likely due to a memory lapse, contributors include: high mental workload; and lack of explicit reminder cues that the condensate booster pumps would come on if not secured (e.g., cues could have been provided in procedures or, as part of advanced control room "significant message" displays that display messages reminding operators of automatic systems that are about to come on).

on low pressure. As described in the human performance study report the operator crew had difficulty determining the source of the RCS pressure decrease. One of the operators intentionally bypassed engineered safeguards in order to gain more time to identify the cause of the pressure decrease. The crew unbypassed the engineered safeguards six minutes later at which point the high pressure injection system activated. The cause of the decrease in RCS pressure remained unknown to the operators until the spray line block valve was closed about an hour later, which stopped the leak.

The NRC human performance study report on the incident identified a number of performance deficiencies. Specifically:

a) Failure to diagnose pressurizer spray flow control valve RCV-14

b) Bypassing engineering safeguards while a plant depressurization was in progress and not diagnosed or understood

c) Securing of high pressure injection system injection flow before the reactor coolant system pressure had risen well above the 1500 psig minimum for the subcooling margin requirements

Brief analysis of the cognitive demands inherent in the situation suggests that contributors to the operator performance deficiencies may have included:

a) Failure to diagnose pressurizer spray flow control valve RCV-14:

- *misleading indicator* – valve position indicator read closed in spite of the fact that the valves were partly open

- *no reason to call this hypothesis to mind* – the pressurizer spray line control valve, RCV-14 had not been opened during this startup prior to this event

- *availability of a hypothesis that could partially account for the symptoms* (at a gross level of behavior – but not if evidence was examined in more detail or if disconfirming evidence sought). The operators hypothesized that RCS was in a cooling transient. This was consistent with a report from the AO that significant steam flow to the deaerating feed tank from the steam generators had been initiated, which would cause the RCS coolant to shrink and lower pressurizer level and pressure; however a more detailed examination of the plant parameters would have indicated that RCS temperatures were only decreasing slightly and that pressurized level was increasing slightly.

- *no relevant procedural guidance.* The annunciator response procedure for low reactor coolant system pressure was oriented toward control circuit failures, which left RCV-14 indicating open; The abnormal response

procedure for engineered safeguards/high pressure injection system actuation had directions for closing the spray line isolation valve RCV-13 to correct a low reactor coolant system pressure condition, but these directions were in a later section of the procedure that was past the procedure exit point.

b) Bypassing engineering safeguards, while a plant depressurization was in progress and not diagnosed or understood.

- There are some conditions under which operators are permitted to bypass these engineering safeguards. According to the incident report these engineering safeguards are bypassed as part of the plant shutdown procedures (as part of a controlled cooldown and depressurization).
- The operator believed that the engineering safeguards bistable trip setpoints are set conservatively
- Engineering safeguards bypass could give him a few more minutes to find and correct the cause of the decreasing RCS pressure
- Engineering safeguards bypass was reversible and could be removed at any time
- Engineering safeguards initiation would have negative economic consequences

c) Securing of high pressure injection system injection flow before the reactor coolant system pressure had risen well above the 1500 psig minimum for the subcooling margin requirements

- *Need to balance multiple safety goals.* HPI flow was stopped because of the operators' concerns about overfilling the pressurizer and lifting the safety valve or power operated relief valve.
- *Lack of procedural guidance for relative priority of goals and/or strategies for simultaneously satisfying the multiple goals.* The procedure did not contain any direction either as to avoiding a relief or safety valve lift or as to favoring an adequate SCM at the expense of a relief or safety valve lift.