APPENDIX A
REPRESENTATIONS OF SELECTED OPERATIONAL EVENTS FROM AN ATHEANA PERSPECTIVE

A.1.1 EVENT IDENTIFIER - Three Mile Island 2

Plant Name:	Three Mile Island 2
Plant Type/Vendor:	PWR/B&W
Event Date/Time:	03/28/79, 04:00
Event Type:	Small-break LOCA with loss of primary cooling
Secondary Event:	Reactor trip with failure of all EFWS
Unit Status:	Full-power
Data Sources:	Three Mile Island Report of NRC's Special Inquiry Group (Rogovin, et al.), January 1980; Analysis of Three Mile Island - Unit 2 Accident, NSAC-1, Nuclear Safety Analysis Center, July 1979 and Supplement 1, October 1979.
Data Input By:	John Wreathall, Contractor (TWWG), 614-791 9264

A.1.2 EVENT SUMMARY

Event Description: Three Mile Island, Unit 2 (TMI-2) experienced a turbine trip and consequential reactor trip because of loss of feedwater. Loss of feedwater occurred because of ingress of moisture to the instrument air system used to control the condensate polishing valves. The moisture ingress came from use of an air lance by plant operators to try to unblock a blocked resin bed transfer line; the air lance was inappropriately connected to the instrument air supply because of its proximity to the resin bed. Following the reactor trip, the emergency feedwater (EFW) system failed to provide cooling to the once-through steam generators because the EFW inlet block valves were closed (probably as a result of a failure in earlier maintenance). The operators were unaware initially that the EFW valves were closed because tags on the control room panel hid the indicators. The primary system pressure rose and caused the pressurizer relief valves to cycle to relieve the high pressure. Shortly thereafter, the pressurizer emergency relief valve (ERV) stuck open. However, the operators were unaware of the valve being stuck open because the position indicator showed the "demanded" position of the valve (whether the control solenoid was energized or not), not its actual position. A second indication of the valve being open (high line temperature) was discounted by the operators since the valve was known to leak.

Because of concerns that the indicated pressurizer water level was indicating high and increasing, the operators became convinced that the reactor primary system was "going solid." That is, the steam bubble in the pressurizer was shrinking to zero, which potentially would mean loss of pressure control of the primary system and the possibility of a loss-of-coolant accident (LOCA) being caused. The operators were from the Navy nuclear program, in which "going solid" is a major area of concern. Because of this concern, the operators throttled high-pressure injection (HPI) virtually to zero injection within 5 minutes of the initiating event. HPI flow was effectively zero for the next 4 hours. Three minutes later, at 04:08, the operators discover the EFW valves closed and opened them, restoring flow to the steam generators. At 04:20 and 04:38, the operators do not recognize the existence of the LOCA when the rupture disk on the reactor coolant drain tank (RCDT) fails and when the containment sump alarms indicate high. At 06:18, the operators close the block valve for the ERV but make no attempt to restore HPI until 08:17. Because of the lack of HPI flow, two-phase flow in the primary system was taking place. By 05:14, the two-phase flow led to serious vibrations in the "B" reactor coolant pumps so the operators stopped the pumps. About 30 minutes later, at 05:41, the operators stopped the "A" reactor coolant pumps because of significant vibration. These pumps remained off until 19:50, when the operators restarted them; thereby, restoring forced cooling within the primary system.

Over the next days, operators and NRC analyzed and responded to concerns of hydrogen build-up in the primary system.

Three Mile Island 2
Small-break LOCA with loss of primary cooling
March 28, 1979

Event Surprises: The operators overlooked the possibility of a two-phase coolant in the reactor coolant system (RCS) for a prolonged period of time despite numerous symptoms of the LOCA, its consequences to the reactor coolant pumps, and core damage shown by the indications of the in-core thermocouples.

Licensee Corrective Actions: The industry and NRC implemented significant changes in the practices associated with the human-factors design of control rooms, the basis for and design of emergency operating procedures, and the industry approach to training.

ATHEANA Summary:
Deviation From the "Expected" Scenario:
- The discharge path via the pressurizer power-operated relief valve (PORV) for the LOCA was unexpected. The consequence of this deviation was that the operators were misled by the indicated increasing pressurizer level to believe that the RCS was going solid.
- In relation to the discharge path, the fact that the indications associated with the PORV were not directly measuring its position, but rather its demanded position, misled the operators into not realizing the valve was open. This discrepancy in information was a significant deviation from expected.
- Complete failure of the emergency feedwater system to start (due to its non-restoration after previous maintenance) on loss of main feed was a deviation from the expected scenario for loss of all feedwater.
- Behavior of the RCS after the saturation point had been reached was a significant deviation from the expected for the operators and the NRC.

Key Mismatch(es):
- The behavior of the RCS indications (particularly of the pressurizer level) compared with the operators' training and procedural guidance for small LOCAs was a mismatch.
- The indicated position of the pressurizer PORV compared with its actual position (both the valve position indicator and the downstream line temperature indications) created a mismatch.
- The relative importance of the risks of the RCS going solid versus the risks from two-phase conditions.
- The belief that the core exit thermocouples were faulty based on the very high readings.

Most Negative Influences
- The operators' **prior experience (PSF)**, particularly their navy training, had created a belief that "going solid" was just about the worst condition that the plant could be in. The TMI **training (PSF)** had not overcome that experience, and the **procedures (PSF)** were not particularly helpful for the situation.
- Many of the indications that might have helped the operators recognize the plant conditions were located such that they were not visible in the normal working areas of the control room (**man-machine interface - PSF**).
- The operators were not trained to recognize the potential for a LOCA via the steam-generator relief valves where the normal symptom of a small LOCA (falling pressurizer level) are reversed (**training - PSF**).
- The problem underlying many of these deficiencies was the failure within the industry to recognize the significance of small-break LOCAs, both in terms of their significance to risk and their differences from design-basis (large) LOCAs in terms of what symptoms might exist and the responses required of the operator (**unexpected plant dynamics - plant condition**).

<u>Most Positive Influences</u> (that could have prevented or otherwise mitigated the event)
- The most positive influence was the involvement of outsiders who eventually identified the appropriate response to the event (**plant condition**).
- In many (though not all) cases, instrumentation existed that could, if seen, have revealed the existence of the LOCA such as the containment sump drains and the pressure in the RCDT. Even the reactor system pressure, if attended to, would have revealed that the reactor coolant was in a two-phase state (**instrumentation - PSF**).

Significance of Event:
This event represents the only accident involving substantial core damage at a U. S. commercial power plant.

Extreme or unusual conditions: None initially. Subsequently, RCS level fell to the point of uncovering the core with resultant fuel damage.
Contributing pre-existing conditions: EFW system isolated probably exacerbated the RCS pressure transient; leaking PORV masked some of the stuck-open valve symptoms.
Misleading or wrong information: PORV position indicated the valve was shut.
Information rejected or ignored: Core exit thermocouple readings were ignored as being faulty.
Multiple hardware failures: Loss of main feedwater system; EFW system isolated; PORV stuck open.
Transitions in progress: Unblocking the resin beds in the feedwater polishing system.
Similar to other events: Symptoms of pressurizer LOCA resembled the RCS going "solid", an event of great concern to the crew from their Navy nuclear experience.

KEY PARAMETER STATUS	
INITIAL CONDITIONS	**ACCIDENT CONDITIONS**
Power level: 97% **RCS temperature (°F)**: Nominal **RCS pressure**: Nominal (about 2255 psig) **RCS level**: Nominal **Other**: Nominal	**Power level**: Tripped **RCS Temperature (°F)**: 590 - 780 **RCS pressure**: 400 - 2365 psi **RCS level**: Minimum ~3 feet above bottom of active core **Other**: Fuel temperatures in excess of 2500°F

FACILITY/PROCESS STATUS	
Initial Plant Conditions & Configurations	**Accident Conditions & Consequences**
Configuration: (1) Nominal at-power conditions (2) Crew was responding to problems in the condensate polishing plant (3) Unit 1 was in hot shutdown **Noteworthy Pre-existing Conditions:** (1) Emergency feedwater block valves closed (2) Pressurizer ERV had a history of leaking, with high line temperature indicated (3) Pressurizer spray valve and heaters were in manual control **Initiator** (1) Turbine trip on loss of feedwater led to reactor trip on high RCS pressure	**Automatic Responses:** (1) EFW system auto-initiated (2) Pressurizer ERV cycled to relieve high RCS pressure (3) High pressure injection pumps 1A and 1C started on low RCS pressure (ESF actuation signal) **Failures:** (1) EFW block valves were closed (assumed a latent failure following earlier maintenance) thereby preventing secondary cooling for initial 8 minutes (2) ERV stuck open

A.1.3 ACTION SUMMARY

Event Timeline:

Pre-Initiator / Initiator / Post-Accident

(-42hr)	up to 04:00	04:00	04:05	05:14	06:22	07:20	19:33
	^ ^ ^	^	^	^	^	^	^
U1	U2	E1	U3	H1	R1	R2	R3

Unsafe Actions and Other Events:
Key: U = unsafe actions
E = equipment failures (significant to the event)
H = non-error (non-recovery) actions
R = recovery actions

UNSAFE ACTIONS AND OTHER EVENTS	
ID	**Description**
U1	EFW block valves left shut (probably from maintenance work 42 hrs before initiating event)
U2	Operators use instrument air to try freeing blocked resin bed transfer line - leads to initiating event
E1	Pressurizer ERV sticks open
U3	Operators throttle HPI "to prevent pressurizer going solid"
H1	Operators shut down RCPs on indication of high vibration
R1	Operators close ERV block valve
R2	Operators manually initiate additional HPI flow
R3	Operators restart RCPs

HUMAN DEPENDENCIES		
ID	**Dependency Mechanism**	**Description**
	None	

Unsafe Actions Analysis		Three Mile Island 2
U1: Unknown, but probably EOO, slip: Valves not restored after maintenance.		
Error Forcing Context		
Plant Conditions	**PSFs**	**Failures in Information Processing**
Evolution and activities: 1) It is assumed that the valves were left closed following earlier maintenance work though the personnel involved in that work reported the valves as repositioned correctly. *Configuration:* 2) Unknown. *Plant Impact:* 1) Prevented initial secondary cooling, which exacerbated pressure transient following loss of feedwater.	Unknown.	Unknown.
U2: EOC: Operators use instrument air (IA) to try to free clogged resin transfer line - moisture entered instrument air supply (could be mistake or circumvention concerning use of IA for non-control purposes but no information provided)		
Error Forcing Context		
Plant Conditions	**PSFs**	**Failures in Information Processing**
Evolution and activities: 1) Operators had been experiencing difficulties in transferring resins from an isolated condensate polisher to a receiving tank. Attempts to free the plugged transfer line had been in progress for about 11 hours.	Unknown.	Unknown.
U3: EOC: Mistake: Operators substantially terminated HPI "to prevent the pressurizer from going solid"		
Error Forcing Context		
Plant Conditions	**PSFs**	**Failures in Information Processing**
Evolution and activities: 1) Operators were responding to the operation of automatic controls in the immediate post-initiator phase. *Configuration:* 1) Plant had tripped on high RCS pressure following loss of feedwater; emergency feedwater injection flow was blocked by the valves left shut (consequence of U1). HPI started injecting automatically. ERV LOCA discharged via pressurizer. *Plant Impact:* 1) Substantially causes core damage.	*Man-machine interface:* 1) ERV position indication was on the basis of "demand" signal, not actual position. Many indications that might have prevented the misunderstanding were located on back panels. *Training:* 1) Operators were untrained in LOCAs via the pressurizer relief lines. 2) Operators persisted in believing that "going solid" was a major hazard at TMI. *Procedures:* 1) LOCA procedures did not provide direct guidance for the ERV LOCA.	*Situation Assessment:* 1) Operators created a mistaken situation model because of the following factors: • pressurizer level indicated high and rising • ERV position indicated the valve was closed when it was open • ERV discharge line had a history of indicating high

A.1.4 ACCIDENT DIAGNOSIS LOG

Time*	Accident Progression & Symptoms †	Response ‡
Just before 04:00	Unit at 97% and nominal conditions. Plant operators were unblocking a condensate polishing bed resin transfer line using instrument air to supply air lance **(U2)**	
04:00:37	Condensate polishing valves closed because of moisture in instrument air supply. Turbine tripped on resulting loss of feed water	
04:00:45	Reactor tripped on high RCS pressure following turbine trip and loss of main feed water	
04:00:49	Pressurizer emergency relief valve (ERV) cycled and then stuck open **(E1)**	None. Control-room indication shows valve shut--signal is "demand" not "actual" position
04:05:15	Pressurizer level was 363" and increasing	Operator throttles HPI flow "to prevent system going solid" - procedures state pressurizer level must not exceed 400" **(U3)**
04:08:55		Operators discover emergency feedwater (EFW) block valves are shut and open them, allowing EFW flow to the steam generators
04:14 - 04:20	Reactor coolant drain tank (RCDT) rupture disk failed	Operators note pressure drop in RCDT but fail to diagnose ERV LOCA
04:25 - 07:??	ERV discharge line temperature high	Operators twice consider this to be the residual heating effect of the initial valve opening
04:38	Containment sump pumps reported running	Operators turn off pumps
04:40+	Low boron measurement plus increasing neutron count in core	Significance not understood (indication of core drying out)
05:00	Containment building temperature is 170°F, pressure is 2.5 psi	Not apparently observed
05:14	Both loop B reactor coolant pumps (RCPs) indicate significant vibration	Operators shut down loop B RCPs (H1)
05:41	Loop A RCPs indicate significant vibration	Operators shut down loop A RCPs **(H1)**

Time*	Accident Progression & Symptoms †	Response ‡
06:18	ERV discharge line temperature high	Operators requested ERV line temperature reading, and closed ERV block valve 4 min later (R1)
06:45 - 06:54		Operators try starting RCPs - pump 2B runs for a few seconds and trips; other pumps do not start
06:55		Site emergency declared
07:13		Operators reopen ERV block valve; ERV line temperature increased
07:17		Operators reclose ERV block valve
07:20		Operators manually initiate safety injection signal, reactor coolant make-up pump 1C starts **(R2)**
07:24	8R/hr radiation reading in reactor building	General emergency declared
08:17 - 08:27	Make-up pumps 1A, 1C tripped	Pump 1B started manually, pump 1C restarted manually
19:33 - 19:50		RCP 1A started manually, stopped, and restarted **(R3)**

* Times are based on NSAC 1 analysis
† A large number of alarms and indications occurred throughout the event, many of which were indicative of the event
‡ Operators performed many actions beyond those listed here which played key roles in the event

A.2.1 EVENT IDENTIFIER - Crystal River Unit 3

Plant Name:	Crystal River Unit 3
Plant Type and Vendor:	PWR/B&W
Event Date, Time:	12/8/91, 2:49 am
Event Type:	Pressurizer spray valve failure
Secondary Initiator:	None
Unit Status:	Start-up
Data Sources:	AEOD/INEL Trip Report, "Onsite Analysis of the Human Factors of an Event at Crystal River Unit 3 December 8, 1991 (Pressurizer Spray Valve Failure)," EGG-HFRU-10085, January 1992
Data Input By:	Leslie Bowen, Contractor, Buttonwood Consulting, Inc., (703) 648-3104

A.2.2 EVENT SUMMARY

Event Description: On December 8, 1991, a reactor coolant system (RCS) pressure transient occurred during startup following a reactor power increase. During a normal power increase the pressurizer spray valve cycled opened to control a slight increase in pressure. The actuator for the spray valve failed which left the valve partly open but position indicating lights showed that the valve was closed. RCS pressure began to decrease and as a result of the erroneous indication, the operators failed to identify the cause. RCS pressure continued to decrease, reaching setpoints for arming the engineered safety features (ES). Circumventing procedural guidance, operators bypassed ESF for 6 minutes, in anticipation of terminating the transient. Control room supervisors directed operators to take ESF out of bypass and the high-pressure injection system automatically started. Injection was secured because of fears of over-filling the pressurizer but eventually the operators reinitiated injection to increase and stabilize RCS pressure. The pressure transient was terminated after the pressurizer spray line isolation valve was closed, on the suggestion from a supervisor that it might be helpful.

Event Surprises: ES Bypass by the operator without understanding the cause of the transient.

Licensee Corrective Actions: At the time of the report, plant management was considering the following types of actions to reduce the reliance on knowledge-based behavior during this type of event:
(1) providing a diagnostic procedure for response to a loss of control of RCS pressure
(2) providing a clearer statement in policies and procedures defining the restrictions on overriding ES actuation or other safety system actuation
(3) reviewing and supplementing existing training fore this type of event.

ATHEANA Summary
Deviation From the "Expected" Scenario:
- Continuing pressure decrease due to stuck open spray valve.
- Instrument failure in an unannounced mode: pressurizer spray valve indicated closed, when it was actually open.

Key Mismatch(es):
- Training (inexperienced crew) not well matched to this unusual plant condition; snap judgment of situation was incorrect, but adopted by entire crew without question. Strong confirmation bias (assumed cooldown confirmed by decreasing pressure, closed indications for PORV and spray valve, and field reports of steam flow to the de-aerators) led to failure to use procedures and failure to notice contradictory evidence.

- Supervision not well matched to the inexperience of crew and the unusual plant conditions, in that supervision did not provide guidance for diagnosis or for which procedures to turn to in the early stages of the event.
- Procedures were a weak match for this particular scenario, in that the scenario was not specifically addressed.

Most Negative Influences:

- Both procedures and training were unclear regarding diagnosis of decreasing system pressure. (PSF)
- There was no indication of spray line flow to use to verify the valve position. (PSF).
- STraining was not sufficient to prevent operators from taking action that was against procedure and policy (bypassing ES). (PSF)

Most Positive Influences:

- That experienced plant management was in the control room to advise in two key instances (1) to unbypass ES and (2) to close the spray isolation valve. (Plant Condition)

Significance of Event:

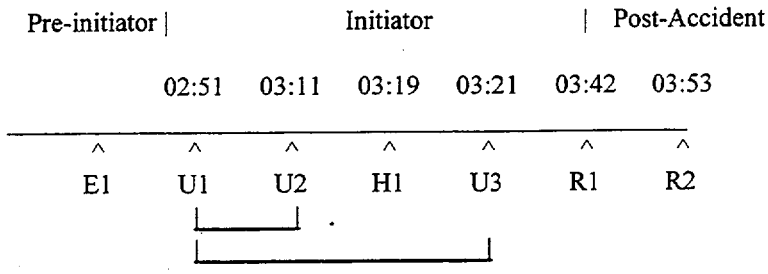
Extreme or unusual conditions: None.
Contributing pre-existing conditions: Shift turnover briefing included mention of spray valve position indicator trouble.
Misleading or wrong information: Pressurizer spray valve indicated closed, when it was really open.
Information rejected or ignored: Briefing on spray valve position indicator trouble.
Multiple hardware failures: None.
Transitions in progress: Power ascension following startup.
Similar to other events: Decreasing pressure believed to be because of pressure outsurge, as a consequence of reactor coolant shrink (as a result of cooldown), despite evidence to the contrary.

KEY PARAMETER STATUS	
Initial Conditions	**Accident Conditions**
Power level: 10% RCS temperature: normal operating temperature RCS pressure: normal operating pressure RCS level: normal level Other:	Power level: 0% RCS temperature: low of 544°F RCS pressure: low of around 1500 psig RCS level: increased to top of scale Other:

FACILITY/PROCESS STATUS	
Initial Plant Conditions and Configuration	**Accident Plant Conditions and Consequences**
Configuration: The plant is starting up from a short maintenance outage. The rods are in manual and the operators are preparing to roll the turbine by increasing reactor power to 15%. The plant lineup is normal configuration for start-up. **Preexisting operational problem:** Shift turnover briefing included mention of spray valve position indicator trouble. **Initiator:** Following a normal increase in reactor power, the pressure control system automatically opened the pressurizer spray valve to compensate for a small increase in pressure.	**Automatic Response:** 1) Reactor trip on RCS low pressure (1800 psig) 2) "ES A and B not bypassed" alarms (1640 psig) 3) ES initiation (1553, 1574 psig) **Failures:** Pressurizer spray valve indication is erroneous in that the pressurizer spray line control valve does not reseat because of a failed actuator but the control board indicator shows it as closed.

A.2.3 ACTION SUMMARY

Event Timeline:



Key:
U = unsafe actions
E = equipment failures
H = non-error (non-recovery) actions
R = recovery actions

UNSAFE ACTIONS ANALYSIS	
ID	**Description**
E1	Spray valve actuator faulty
U1	Operators increase power to increase Tave and RCS pressure.
U2	Operators bypass ES
H1	Operators unbypass ES
U3	Operators secure HPI
R1	Operators take manual control of high-pressure injection to stabilize RCS pressure
R2	Operators close the spray line isolation valve.

HUMAN DEPENDENCIES		
Actions	**Dependence Mechanism**	**Description**
U1, U2	Training	Operator did not refer to procedures
U1, U3	Situation Assessment	Incorrect mental model influenced use of available information to reach the correct conclusion

Unsafe Actions Analysis — Crystal River 3

U1 EOC, Mistake Operators increase reactor power (several times) to increase RCS temperature and pressure.

Error Forcing Context

Plant Conditions	Performance Shaping Factors	Failures of Information Processing
Evolution and activities: 1) The plant is starting up from short maintenance outages. The rods are in manual and the operators are preparing to roll the turbine by increasing reactor power to 15%. *Configuration:* 1) The plant lineup is normal configuration for start-up. *Preexisting operational problems:* 1) Shift turnover briefing included mention of spray valve position indicator trouble. *Plant Impact:* 1) RCS pressure decrease with resulting reactor trip and high-pressure safety injection	*Procedures:* 2) Procedures were not used. Had they been, they may not have helped the diagnosis. *Training:* 1) Operators relatively inexperienced in responding to unplanned transients. Operators did not turn to procedures. *Supervision:* 1) Supervision did not provide guidance in diagnosis or to turn to the procedures in the early stages of this event. *Stress:* 1) Plant dynamics provided limited time for investigation , analysis, and decision-making. *Environment:* 1) Significant actions during the event took place between 3:00 am and 4:00 am. (Effect of duty rhythm is expected to impact cognitive capabilities more than skill- or rule-based activities.	*Situation Assessment:* 1) Action on the basis of incorrect conjecture that an overcooling event was in progress. This conjecture seemed to be supported by reports from field operators that there was steam flow to the deaerators although securing the flow did not change the plant response. 2) Although operators were monitoring pressurizer parameters, the evidence that level remained fairly stable and T_{ave} was decreasing only slightly did not cause a reanalysis of the situation model the operators were holding. *Response Planning:* 1) Operators did not refer to procedures, in particular not to the annunciator response procedure which would have been appropriate. 2) In actuality, the annunciator response procedure did not provide guidance that would have assisted in stopping the pressure decrease.

U2 EOC, Mistake Operators bypass ES

Error Forcing Context

Plant Conditions	Performance Shaping Factors	Failures of Information Processing
Safety equipment actuation: 1) Reactor trip on RCS low pressure (1800 psig) 2) AES A and B not bypassed@ alarms (1640 psig) *Indications:* 1) Pressurizer spray valve indication malfunction *Plant Impact:* 1) Pressure continues to decrease and threatens sub-cooling margin	*Procedures:* 1) Procedures were not used. Had they been, they may not have helped the diagnosis. *Training:* 1) Operators did not use procedures and violate procedures by bypassing ES without an understanding of what was causing the transient. Operators terminate HP flow because of concerns with taking the pressurizer solid without benefit of procedure. 2) Communications: *Supervision:* 1) Supervision did not provide guidance in diagnosis or to turn to the procedures in the early stages of this event. *Stress:* 1) Plant dynamics provided limited time for investigation , analysis, and decision-making. *Environment:* 1) Significant actions during the event took place between 3:00 am and 4:00 am. (Effect of duty rhythm is expected to impact cognitive capabilities more than skill- or rule-based activities.	*Response Planning:* 1) Operator does not refer to procedure when bypassing ES. Bypassing ES is in error. 2) Operator does not seek permission from nor inform supervision of ES bypass.

U3 EOC, Mistake Operators secure HPI

Error Forcing Context

Plant Conditions	Performance Shaping Factors	Failures of Information Processing
Safety equipment actuation: 1) Reactor trip on RCS low pressure (1800 psig) 2) AES A and B not bypassed@ alarms (1640 psig) 3) ES initiation (1500 psig) *Indications:* 1) Pressurizer spray valve indication malfunction *Plant Impact:* 1) RCS pressure decreases and threatens sub-cooling margin	*Training:* 1) Procedure for securing ES is followed without understanding nature of the transient. *Supervision:* 1) Supervision did not provide guidance in diagnosis or to turn to the procedures in the early stages of this event. *Stress:* 1) Plant dynamics provided limited time for investigation , analysis, and decision-making. *Environment:* 1) Significant actions during the event took place between 3:00 am and 4:00 am. (Effect of duty rhythm is expected to impact cognitive capabilities more than skill- or rule-based activities.	*Situation Assessment:* 1) Operators shift concern from decreasing pressure to overfilling the pressurizer. *Response Planning:* 1) Operators do not continue with the ES actuation procedure once conditions for securing the HPI are met. Later instructions would have them isolate all sources of low RCS Pressure including closing the spray isolation valve.

A.2.4 ACCIDENT DIAGNOSIS LOG

Time	Accident Progression and Symptoms	Response
24:39	Reactor Startup	
1:03	Reactor Critical	
2:07	Entered Mode 1 operations; power above 1% Warmed steam lines, established main condenser vacuum, and dumping steam to the main condenser via turbine bypass valves (TBVs)	
2:47	Reactor power increased from 1% to 12%	NO2 pulled rods to increase reactor power; NO1 preparing to roll turbine
2:49	Reactor pressure increased slightly in response to small power increase which caused spray valve to actuate, but did not reclose.	NO2 reported that the RCS pressure was decreasing. NO1 suggested that NO2 bump up power to increase reactor temperature.
2:51	Reactor power increased to 14%. RCS pressure increased 2223 psig and then began to decrease. Tave was 567.3°F and pressurizer level was 176 in.	U1: Operator pulled rods to increase reactor power by 3%.
2:52	RCS Pressure was 2150 psig and decreasing; Tave was 568.5°F and pressurizer level was 190 in.	NO2 monitoring parameters on the strip chart recorders on the panels. NO1 was monitoring RCS pressure on the digital indication available on the safety parameter display systems (SPDS).
2>53	RCS low pressure alarm annunciated.	Operators began a concerted search for the cause of the decreasing RCS pressure transient. Secured steam flow to deaerating feed tank on the premise that an RCS cooldown was in progress. Checked for indications of LOCA. ANSS suspected (incorrectly) that the insurges to the pressurizer caused by reactor power bumps were cooling the water in the pressurizer and decreasing the pressurizer temperature and pressure. Operators manually closed pressurizer spray control valve to ensure that it was closed even though the indication was that it was already closed.
2:54	RCS pressure was 2050 and decreasing.	U1: NO2 bumped reactor power 3% to 15%.
3:00	RCS pressure was 1980 and decreasing.	U1: NO2 bumped reactor power from 13.5% to 15%.
3:09	Reactor auto trip on RCS low pressure (1800 psig); Low pressurizer level alarm annunciated.	Operators entered reactor trip procedure AP-850. Immediate actions were being executed.
3:11	ES A and B Not Bypassed alarms at 1640 psig	U2: NO1 bypassed both A and B HPIS and alarms cleared.
3:12		NO1 announced that ES A&B were bypassed.
3:19	ES initiation bistables tripped. RCS pressure at 1553 psig on Channel A and 1574 psig on Channel B.	AOS asked ANSS and the SS if they concurred with the ES bypass. ANSS directed that the bypass be lifted.
3:19:04	HPI initiated, EFW initiated. DG started.	H1: NO 1 removed the bypass. Operators entered ES actuation procedure AP-380.
3:20		NO1 bypassed ES as per procedure and secured EFW, as normal feed was available.
3:21	RCS pressure increased to 1600 psig.	U3: NO1 secured flow from the HPIS into the RCS and stopped pumps 3A and 3C leaving 3B running.
3:27	RCS pressure increase reset the 1500 psig bistables for auto ES initiation.	NO1 reset auto initiation circuit.
3:35	RCS pressure began to decrease again and decreased sufficiently to trip on 1500 psig ES bistable.	NO1 bypassed the automatic ES initiation
3:42	RCS pressure continues to decrease. RCS temperature has decreased to 544°F but has begun to increased once ES was secured.	Operators monitoring the subcooling margin indication. R1: ANSS decided to prevent RCS pressure form decreasing below 1500 psig by establishing a controlled HPI flow to the RCS to increase water level and compress the bubble, thereby increasing pressure. ANSS directed NO1 to slowly open makeup valve MUV-24. HPI pump 3B was still operating. NO1 does as directed.

Crystal River 3
Pressurizer Spray Valve Failure
December 8, 1991

Time	Accident Progression and Symptoms	Response
3:42	RCS pressure begins to increase slowly from 1503 psig.	
3:45	Pressurizer high level alarm annunciated. RCS pressure was 1550 psig.	
3:53	RCS pressure at 1675 psig and pressurizer level indication was at the top of the scale.	**R2**: AOS suggested that the pressurizer spray line isolation valve be closed.
3:54	RCS pressure began to increase rapidly.	Operators take manual control of the pressurizer heaters.
4:02	RCS pressure stabilized at approximately 1750 psig.	
4:55		SS made an emergency action level determination of an unusual event.
5:00		State notification
5:06		SS declared that the event had been exited.
5:32		NRC notification.

A.3.1 EVENT IDENTIFIER - North Anna 2

Plant Name:	North Anna 2
Plant Type and Vendor:	PWR/W
Event Date, Time:	4/16/93, 7:16 am
Event Type:	Degradation of heat removal capability by disabling AFWS (i.e., bypass of ESFAS)
Secondary Initiator:	None
Unit Status:	Full power
Data Sources:	LER #93-002-00 dated 5/14/93; Inspection Report 50-339/93-17 conducted 4/16-23/93; AEOD/INEL Trip Report, "Disabling of Auxiliary Feedwater System (AFWS) During Reactor Trip Recovery," 6/93
Data Input By:	Alan Kolaczkowski, Contractor, SAIC, (303) 273-1239

A.3.2 EVENT SUMMARY

Event Description: The unit experienced an automatic generator-turbine-reactor trip because of a failed voltage regulator. Safety systems responded as designed although there were other nuisance failures. Approximately 9 minutes into the event, an operator, without explicit knowledge of shift supervision, disabled the entire AFWS (which was running) and used main feedwater (which was recirculating at the time) as a means to feed the steam generators and control primary plant cooldown (operator was concerned about excessive cooldown with full AFWS flow). A valid AFWS start signal from low-low steam generator levels in all 3 steam generators was still present. This condition was not recognized until about 18 minutes after the AFWS was disabled during a procedural step for recovering all systems back to a "normal" state. The AFWS was then returned to "auto" standby per direction of shift supervision. Main feedwater had already recovered all 3 steam generator levels. Further shutdown of the unit proceeded normally.

Event Surprises: No one noticed the disabling of AFWS in spite of turbine AFWS steam valves closed alarms and other visual indications (motor AFWS pump controls in pull-to-lock, operator using main feedwater).

Licensee Corrective Actions: Subsequent actions included:
(1) Unit 2 Supervisor and Backboard operator relieved of license duties and coached on station's policy for defeating ESFs as well as later received remediation training on control room communication and control room command and control structure.
(2) Requirements put in place to discuss event in Licensed Operator Requalification program.
(3) "Nuisance" hardware problems repaired.
(4) Root cause and other actions - pending management review. (Do not know what else was done)

ATHEANA Summary
Deviation From the "Expected" Scenario:
- The fact that both AFWS and main feedwater were apparently available instead of the "expected" total loss of main feedwater, was a deviation in the scenario that contributed to the unsafe act of most concern.

Key Mismatch(es):
- How to handle the situation when both AFWS and main feedwater were apparently available, represents the most significant *mismatch* between the actual event and the procedural and training guidance for the operators, (i.e., the

guidance was not clear on how to respond to a rapid cooldown event with both AFWS and main feedwater available).

Most Negative Influences:

- Both procedures and training were unclear (PSFs) as to how to mitigate a rapid cooldown (Plant Condition), particularly when both AFWS and main feedwater are apparently available (Plant Condition).
- Inadequate command and control during the event including directions by multiple persons, closed-loop communications not used, and terminology misunderstanding ("secure" AFWS) (PSFs).
- Operator's pre-conceptions about (a) possible degradation of AFWS pumps when in recirculation, and (b) the best standby status for AFWS (thought it best to have pumps shutdown than valves throttled way down) (PSF).

Most Positive Influences:

- Station policy and licensed operator training address disabling ESFs (PSFs).
- Procedure for returning systems to "normal" caught the fact that AFWS had been inappropriately disabled (PSF).

Significance of Event:

Extreme or unusual conditions:

- Plant configuration ended up such that backup heat removal (AFWS) could not have automatically responded if main feedwater had not restored SG levels or if main feedwater had failed later (i.e., all secondary heat removal would have been lost without manual intervention to "re-enable" AFWS which may or may not have restarted).
- Main feedwater status and operability was not "completely clear" following the initial transient:
  (a) there was a feedwater heater relief valve stuck-open and so the feedwater heater was being isolated (could have disrupted main feedwater flow if subsequent problems occurred),
  (b) "B" main feedwater pump breaker was inoperable in the control room,
  (c) a condensate recirculation valve had failed, and
  (d) a severe weather alert had just been issued (possible jeopardy to offsite power and hence main feedwater operation).

Contributing pre-existing conditions: None

Misleading or wrong information: Control room command and control problems, particularly those related to misunderstanding about the actual status of the AFWS, could have been a more significant factor in more complex or challenging events.

Information rejected or ignored: None

Multiple hardware failures: None

Plant transition in progress: None.

Similar to other events: None.

KEY PARAMETER STATUS	
INITIAL CONDITIONS	**ACCIDENT CONDITIONS**
Power level: 100%	Power level: tripped, headed toward shutdown
RCS temperature: normal operating temperature	RCS temperature: reached min Tavg = 540°F (below no-load control setpoint of 547 ° F)
RCS pressure: normal operating pressure (about 2235 psig)	RCS pressure: minimum reached was 1925 psig
RCS level: normal level	RCS level: minimum reached was 23%
Other: nominal	Other: cooldown rate was about 2F/5 minutes; at time of AFWS disabled, steam generator levels at 5%, 12%, and off-scale low - all below 18% setpoint for auto AFWS start - operator had opened 2 main feedwater bypass valves to supply flow.

FACILITY/PROCESS STATUS	
Initial Plant Conditions and Configuration	**Accident Plant Conditions and Consequences**
Configuration: (1) Nominal at-power conditions. (2) Crew consisted of 3 senior licensed operators and 3 operators; on day 2 (07:00-19:00 shift) following 6 days off; STA also on shift. Crew consisted of Shift Supervisor, Unit 1 Supervisor, Unit 2 Supervisor, Unit 1 reactor operator, Unit 2 reactor operator, and backboard operator. Unit 1 Supervisor came over to Unit 2 side of control room following Unit 2 trip, to assist. **Preexisting operational problem:** No specific equipment or indications noted as being out-of-service or problematic; nor mention of specific administrative controls or temporary equipment in use. **Initiator:** Following a VARS alarm because of a voltage regulator failure, in response to which the Unit 2 reactor operator attempted to take manual control and lower excitation, a differential lockout was received causing a generator-turbine-reactor trip; thereby, starting the event.	**Automatic Response:** (1) 2 condensate and 2 main feedwater pumps remained on-line, recirculating thru 1" line back to condenser (2) All 3 AFWS pumps (2 motor, 1 turbine) auto started with discharge valves full-open on steam generator levels reaching lo-lo setpoint of 18%; flow reached >1400 gpm (3) AMSAC initiated (SG levels <13% in 2/3 SGs); all SG levels continued to shrink (not unexpected) No safety injection ever occurred **Failures:** (1) Abnormal amount of steam in turbine building because of feedwater heat exchanger relief valves lifting and one would not reset - involved Shift Supervisor attention a few times while in the control room to dispatch others and communicate with other operators (2) One control rod bottom indication not reached - Unit 2 reactor operator agitated indicator which broke the cover but caused bottom indication to indicate on the panel. (3) Reactor coolant pump vibration alarm received - responded to by Shift Supervisor who reset alarm and alarm cleared (4) Others: air ejector hi rad spike alarm, "B" MFW breaker light out in control room, condensate recirc. valve failure, source range indication failure. **Consequences:** (1) No plant or offsite damage, or personnel injury occurred; nor was radiation released.

A.3.3 ACTION SUMMARY

Event Timeline:

```
Pre-initiator |          Initiator          | Post-Accident

      07:16                                   07:24  07:26        07:45
_____________________________________________________________________________

      ^ ^                                     ^    ^             ^
      E1 H1                                   U1 U2              R1
                                              |___|
```

Key:
U = unsafe actions
E = equipment failures
H = non-error (non-recovery) actions
R = recovery actions

UNSAFE ACTIONS AND OTHER EVENTS	
ID	**Description**
E1	Exciter field voltage regulator failure cause overexcitation
H1	Operator attempts to manually lower excitation; but plant trips
U1	Operator resets AMSAC although this was not yet directed by procedure (action allows U2)
U2	Operator disables AFWS while AFWS start signal still present (switched to main feedwater)
R1	Crew recognizes AFWS is disabled and restore AFWS to auto start configuration

HUMAN DEPENDENCIES		
Actions	**Dependence Mechanism**	**Description**
U1, U2	Common PSFs and same overall situation assessment.	Operator recognition that U1 was required to be performed in order for U2 to be performed. Taken together, they resulted in the desired (but unsafe) outcome (i.e., really 2 steps in the same single unsafe act of securing AFWS)

Unsafe Actions Analysis — **North Anna 2**

U1 & U2; EOCs; Mistakes (completely coupled)

Error Forcing Context

Plant Conditions

Evolution and activities:

1) The plant was at 100% power with nominal conditions when overexcitation caused plant trip followed by normal response of isolation of main feedwater on low T_{avg} and auto start of AFWS.
2) AMSAC logic tripped when SG levels dropped below 13% before AFWS could recover SG levels (not unexpected).
3) SG "B" level was at 12% and recovering and so had cleared 11% setpoint to allow AFWS flow to be throttled to 400 gpm.
4) SG "A" level at 5%; SG "C" level narrow range off-scale low
5) All AFWS pumps on with discharge valves full open and system supplying >1400 gpm. AFWS valid signal still present since all SGs still <18%.
6) Main feedwater recirculating.
7) RCS conditions indicative of cooldown concerns; though not an extreme cooldown.
8) Other "nuisance" failures were being dealt with

Configuration:

1) Nominal at 100% power and during initial response to trip.

Preexisting operational problems:

1) None indicated.

Plant Impact:

1) U1 allowed AFWS pumps to be stopped even though AFWS start signal was still present (pumps would not stop if AMSAC had not been reset). U2 action then disabled AFWS such that it could not have auto restarted if main feedwater had subsequently not worked or failed. Because main feedwater did successfully operate and restore SG levels, the heat sink was never actually lost.

Performance Shaping Factors

Procedures:

1) Procedure not clear as to how to mitigate a cooldown beyond step 1, which occurred in this case. No procedural direction on shutting down AFWS and placing main feedwater in service.

Training:

1) Topic of overriding or disabling ESFs is an integral part of licensed operator training.
2) Unclear as to design basis of AFWS with SG levels between 11% and 18%. Previous training had not prevented Backboard operator's rendering AFWS inoperable when permission received to use main feedwater. Previous training for all operators had not established consistent procedure usage for stopping a cooldown event and in fact usually dealt with events where the need to cooldown was req'd.

Communications:

1) "Secure" AFWS thought to mean to close AFWS valves to reduce flow by SS and Unit 2 Supervisor (terminology problem). Procedure reader (Unit 1 Supervisor) not included in command path to ensure procedure properly carried out. Multiple supervisors (SS, 2 Unit Sups) giving commands at various times. Closed-loop communications not used.

Supervision:

1) Station policy exists on bypassing ESFs.

Staffing:

1) Unit 2 reactor operator had been on the shift for only 2 months. Unit 2 Supervisor had just returned from several months on Unit 1 outage.

Human-System Interface:

1) Multiple indications available in CR of AFWS pump and valve status (two red annunciators, pull-to-lock handles, and valve indicators).
2) STA unaware of specific AFWS status since AFWS pump and valve status not on SPDS safety function pages he was monitoring.

Organizational Factors:

1) No apparent corporate factors involved but specific control room command organization broke down when multiple supervisors gave instructions and closed-loop communication not used effectively. See "Communications" above.

Stress:

1) Concern about cooldown, dealing with other nuisances, and an awareness of accumulation of people in back of CR after trip may have contributed to stress.

Environment:

1) (apparently not a factor)

Other:

1) Backboard operator concerned with use of 1" AFWS recirc line and just throttling back the pumps because of previous pump degradation problems in tests (per follow-up interview). Engineering had "okayed" use of 1" line for short emergency operation but apparently this had not been communicated to everyone. Backboard operator (per interview) apparently also thought that restart timing and reliability of AFWS pumps would be better than stroke-time and reliability of AFWS valves should system have to be restarted. Finally, apparently Backboard operator did not know (understand) that lo-lo SG levels are an ESF.

Failures of Information Processing

Situation Assessment:

1) Apparently failed to recognize that cooldown rate, while of concern, was not excessive which may have contributed to some urgency to fully stop AFWS on part of Backboard operator.
2) Backboard operator believed AFWS recirculation on 1" line may be detrimental to pumps despite Engineering "okay".
3) Backboard operator believed better to restart AFWS pumps than to reopen throttle valves, if necessary.
4) Miscommunication about "secure AFWS" left two different situation assessments in minds of crew concerning status of AFWS (pull-to-lock vs. throttled down).
5) Apparent lack of recognition by Backboard operator that lo-lo SG signals is an ESF that should not be bypassed.

Monitoring and Detection:

1) No one noticed alarms or other visible indications that AFWS had been disabled for 18 minutes.
2) Perhaps other nuisance problems contributed to this lack of detection.
3) No indication of AFWS pump and valve status on SPDS functional displays being used by STA.

Response Planning:

1) Lack of a well-trained plan for how to deal with further evidence of cooldown when past step 1 in procedure.
2) Lack of a well-trained plan for when and how to remove control from AFWS and go on main feedwater especially when heat sink had been re-established but AFWS start signals not yet completely cleared.

Response Implementation:

1) Lack of well-structured line of command during event; may have been contributed to by (a) dealing with other nuisances, and (b) some recent changes to crew.
2) Lack of "closed-loop" communication which may have otherwise "caught" error made by Backboard operator.
3) Apparent lack of knowledge by everyone as to correct time to reset AMSAC.

A.3.4 ACCIDENT DIAGNOSIS LOG

Time	Accident Progression and Symptoms	Response
07:16	Unit at 100% and nominal conditions. Crew being briefed in Tech Support Center adjacent to control room (had just come on shift starting at 07:00). Unit 2 Supervisor on phone with dispatcher about a severe weather alert that had just been issued.	
07:16:28	Exciter field forcing annunciator and a Volts/Hertz relay actuation annunciator received indicating a voltage regulator problem and overexcitation.	**H1:** Unit 2 reactor operator responds and attempts to manually lower excitation.
07:16:45	Differential lockout received causing a main generator trip concurrent with a turbine trip, followed immediately by a reactor trip. Main feedwater isolation subsequently occurs because of Tavg < 554 °F with reactor trip.	Unit 2 Supervisor immediately terminates phone call, locates Procedure "Reactor Trip and Safety Injection," and directs operators to perform immediate actions. Unit 1 Supervisor announces trip over page system and proceeds to Unit 2 side of control room to assist as "procedure reader." Backboard operator leaves Unit 1 side of control room and takes over secondary plant responsibilities for Unit 2. Shift Supervisor and rest of crew take positions and perform immediate actions. STA enters about 1 min. later.
07:16:51	All three AFWS pumps auto start on SG lo-lo levels (<18%). AFWS total flow rate reaches 1425 gpm. Two condensate and two main feedwater pumps running with recirculation thru one line back to condenser. Apparently another recirc line path is failed. Tavg is approaching 547 °F no-load setpoint.	
07:17:19	AMSAC initiates (SG levels <13% in 2 of 3 SGs). All SG levels continue to shrink below narrow range indication	
07:17 - 07:24	Crew notes no safety injection has occurred nor required. Tavg continues to drop Unidentified person pages control room about abnormal steam in turbine bldg. (relief valves on feedwater heat exchangers were lifting and one had stuck-open). Nuisances: One control rod bottom position not indicating. Air ejector high rad alarm received. Reactor coolant pump vibration alarm received.	Crew exits "Reactor Trip and Safety Injection" procedure at step 4 and enters "Reactor Trip Response" procedure. STA checks SPDS and reports to SS and Unit 2 Supervisor that the only function that is not "green" is heat sink condition (SG levels <11% with feed flow >400 gpm) - a yellow condition. • SS dispatches an auxiliary operator (AO) to check on steam in turbine bldg. A few minutes later, AO returns about relief valve and SS dispatches others to isolate feedwater heaters and locally unisolate another main feedwater recirc path. SS, and Unit 2 reactor operator, deal with nuisances (appear to be momentary distractions) as time permits. Unit 2 reactor operator voices concerns several times about decreasing Tavg but gets little or no verbal feedback. He increases charging flow to maintain pressurizer level and watches pressure.
07:24 - 07:26	RCS parameters approaching min values reached during event. SG levels start to recover.	Backboard operator, hearing Unit 2 reactor operator concerns about Tavg, informs Unit 2 Supervisor that SG "B" narrow range level >11% and per step 6 of procedure, AFWS flow can be decreased below 400 gpm. **U1:** Back board operator requests permission from Unit 2 Supervisor to "secure AFWS" and go on main feedwater and that AMSAC be reset - Unit 2 Supervisor directs Unit 2 reactor operator to reset AMSAC which is done. Procedure reader (Unit 1 Supervisor) tries to go back to step 1 in procedure for instructions to control or throttle AFWS even though step 1 is not a continuous action step. Unit 2 Supervisor halts procedure reader. A conference is held among Unit 2 Supervisor, SS, and another SRO from previous shift noting cooldown not that severe. Unit 2 Supervisor then gives permission directly to Backboard operator to "secure AFWS".

Time	Accident Progression and Symptoms	Response
07:26 - 07:27	AMSAC has been isolated (which allows AFWS pumps to be stopped). SG levels: A: 5%; B: 12%; C: narrow range off-scale low (all less than 18% thereby indicating a sustained AFWS start signal). One source range indication not functioning.	**U2:** Backboard operator, without telling anyone and without interaction from procedure reader, opens 2 main feedwater bypass valves to establish flow to SGs and pulls-to-lock AFWS motor pumps and closes 2 steam supply valves to turbine AFW (system now disabled). [Red alarms are present for 2 steam supply valves but *apparently* no one notices or *perhaps* alarms are cleared too quickly]. At this time, Unit 2 Supervisor checks out problem with source range indication and tells Unit 2 reactor operator to enter "Malfunction of Source Range Instrumentation" procedure.
07: 30:38	SG "B" lo-lo level alarm clears (18%)	
07:40:45	SG "C" lo-lo level alarm clears (18%)	
07:43:55	SG "A" lo-lo level alarm clears (18%)	
07:45	All parameters recovering or stable. All SG levels now >20%. Step 12 of procedure is reached which directs shutdown of AFWS.	**R1:** At procedure step 12 which addresses returning AFWS to normal, procedure reader notes AFWS is already in pull-to-lock and immediately notifies SS who directs Backboard operator to return AFWS to auto. This is done (pumps put in auto and steam valves opened).
08:30	Nominal conditions.	Transition to unit shutdown procedure.
09:30	Shutting down.	Post-trip review initiated.
10:55	Shutting down.	NRC notified of reactor trip and the disabled AFWS during the trip recovery.

A.4.1 EVENT IDENTIFIER - Salem 1

Plant Name:	Salem 1
Plant Type and Vendor:	PWR/W
Event Date, Time:	04/07/94, 10:47 am
Event Type:	Loss of Circulating Water
Secondary Initiator:	Loss of Condenser Vacuum
Unit Status:	Full-power
Data Sources:	AIT. 50-272/94-80 and 50-311/94-80
Data Input By:	Susan Cooper, SAIC and Leslie Bowen, Buttonwood Consulting, Inc.

A.4.2 EVENT SUMMARY

Event Description: The plant was at reduced power because of reductions in condenser cooling efficiency resulting from river grass interference with the condenser's circulating water (CW) intake structure. Shortly after 10 am, a severe grass intrusion occurred and many CW pumps tripped. Operators reduced plant power (1%, 3%, 5%, finally a rapid 8%) through manual rod insertion and boration to take the turbine off line. Because of operator errors and pre-existing hardware problems, a reactor trip and safety injection (SI) occurred. As a result of operator errors, the pressurizer filled to solid or nearly solid conditions and PORVs opened numerous times (and normal pressure control was lost). Because of operator error and pre-existing hardware problems, the secondary pressure increased concurrently with pressurizer level, steam generator code safety valve(s) lifted and caused a rapid depressurization, a second SI, and more PORV openings.

Event Surprises:

(1) Control rods were being controlled manually (automatic control out of service because of corrective maintenance) during a period of at least twice daily demands for power reductions.
(2) Caused RT through series of actions: rapid power reduction (manual rod insertion and boration resulting in power reduction up to 8% per minute), over-cooling, then power increase to "reactor startup" 25% power trip setpoint. 3)
(3) Extensive efforts and plans to avoid plant trip (e.g., special procedures and personnel, atypical power reduction, SNSS leaving CR to attempt CW pump restart) but no parallel efforts or plans to address increased workload in control room and no criteria for when to trip reactor.
(4) Spurious SI because of recognized but uncorrected, pre-existing hardware design problem.
(5) RCS overcooling pre-trip, as a result of human actions.
(6) Solid PRZR conditions caused by human actions. Failed to terminate SI early enough to avoid solid PRZR conditions.
(7) Multiple (>300), successful operations of both PORVs.
(8) Failed to monitor and control secondary pressure, resulting in SG code safety valve(s) lifting, rapid depressurization, and second SI (on low PRZR pressure).
(9) Failure of automatic SG pressure control because of recognized but uncorrected, pre-existing hardware problem.
(10) Rapid depressurization and second SI as a result of human actions.
(11) Yellow path, functional recovery procedures not used to re-establish PRZR bubble; rather, plant cooldown achieved through assistance of Tech Support center and manual control of SG atmospheric RVs and letdown and charging.

Licensee Corrective Actions:
(1) Replaced both PORVs.
(2) Made a number of changes and replacements in the steam flow control systems and other steam flow control changes had been planned for upcoming feedwater system modification
(3) Replace summator module in high steam flow setpoint change circuitry with correct model, though did not solve problem the unneeded setpoint drop after reactor trip.
(4) Rod control system isolators replaced to eliminate noise which caused unexpected rod insertion and operators were trained not to use the Tavg recorder as an indicator of required rod speed during power changes.
(5) Procedure changes are referred to but not listed in the report.

ATHEANA Summary

Deviation From the "Expected" Scenario:
- Continuing grass intrusion event combined with unavailability of automatic rod control. Required manual control of reactor power in response to rising condenser back-pressure.
- Degradation of circulating water required 12 people at the intake structure, reducing manning level in control room. Circulating water pump failures forced rapid power reduction and consequential cooldown, to the point reactor trip setpoints dropped to startup settings.
- Spurious and partial safety injection (SI) caused unfamiliar plant response.

Key Mismatch(es):
- Mismatch between operator expectations of unfolding sequence of events and actual plant conditions. Anticipating circulating water recovery, operators focused there and lost control of overall event.
- Mismatch between workload, especially communications flow, and the ability of operators to track changing plant conditions and develop response plans.
- Mismatch between communications goals and practice. With some operators acting independently, there was a consequent loss of supervisory control.
- Complexity and speed of event evolution went beyond training and procedural support.
- Mismatch between operator mental model and the partial SI.

Most Negative Influences:
The operators inability to diagnose the condition of the plant at several junctures, because of training (PSF) in combination with the unavailability of systems and components to operate automatically as designed (Plant Condition).

Most Positive Influences:
In large measure, the plant responded to operator actions as designed, with the exception of the unavailable automatic functions of some systems and components (Plant Conditions). In addition, the operators used EOPs well (Procedures).

Significance of Event:
Extreme or unusual conditions: Severe grass intrusion.
Contributing pre-existing conditions: Operating at reduced power because of marsh grass accumulation on traveling screens. Automatic control rod system out-of-service.
Misleading or wrong information: None.
Information rejected or ignored: Unable to keep up with the flow of information on changing plant.
Multiple hardware failures: Failure of all CW pumps because of grass intrusion , SG atmospheric relief valve (RV) failure as a result of pre-existing problems, spurious SI because of pre-existing design problems, and failure of 12A DW pump to start (circuit breaker not fully racked in).
Transitions in progress: Power reduction in response to decreased circulating water flow.
Similar to other events: History of annual grass problems.

KEY PARAMETER STATUS	
INITIAL CONDITIONS	**ACCIDENT CONDITIONS**
Power level: 73% RCS temperature: Nominal 547°F RCS pressure: Nominal 2235 psig RCS level: Nominal Other:	Power level: 0% RCS temperature: 552°F (high), 531°F (low) RCS pressure: approximately 2300 psig, low of 1755 psig RCS level: Other: Pressurizer solid. The PRT rupture disk relieved to containment as designed during the event.

FACILITY/PROCESS STATUS	
Plant Conditions and Configurations	**Plant Conditions and Configurations**
Configuration: (1) Continuous monitoring of condenser back pressure (and corresponding decrease in power) because of river grass interference w/ circulating water (CW) traveling screens. (2) Rods in manual control (3) Special work control procedures to facilitate quick restoration of failed CW screen shear pins. **Preexisting operational problem:** (1) Operating at reduced power because of reductions of condenser cooling efficiency (result of river grass intrusions at the condenser's CW intake structure). (2) Grass intrusions @ CW intake structure, at least 2 per day (seasonal occurrence, severe attacks in spring and autumn - vulnerability documented for a number of years). (3) Spurious high steam flow signals because of a design which cause spurious SI (first identified in 1989). (4) Problems w/ SG atmospheric RV controllers (since controllers were modified in the late 1970's). (5) The SS and two off-duty SS, the maintenance supervisor, and ~12 people stationed at the CW intake structure w/ fire hoses and shovels during grass intrusions and to assist in pump priming operations. (6) Local SS provided direct continuous communications with both Salem control rooms. (7) Automatic control rod control system (because of CM - out of service for ~1 month before event, final surveillance test needed to return to service scheduled for the day of the event). (8) 12A CW pump out of service for water box cleaning. **Initiator:** (1) Unit 1 operating crew initiated a plant power reduction, at a rate up to 8% per minute, to respond to circulating water system failures.	**Automatic Response:** (1) PRZR heaters cutout on low PRZR level (level contracted to 17% because of overcooling pre-trip). (2) RT on low power high flux at 25% power ("startup"). (3) SI (twice) - "A" only 1st SI, spurious high steam flow + low T_{ave}; "B" only 2nd SI, low PRZR pressure; injection equipment starts in both cases. (4) PRZR level control system tries (but fails) to maintain level by limiting letdown and increasing charging. (5) 2 PORVs together actuated over 300 times. (6) SG atmospheric RVs (not successfully). (7) SG code safety valves. **Failures:** (1) Spurious SI (1st) as a result of pre-existing design problem. (2) Not all safety equipment actuates (e.g., 2/4 MS isolation valves) on 1st SI because of short duration of signal. Manual positioning of 10 valves required. (3) SG atmospheric RVs did not operate as designed to control SG pressure. (4) Controls for 1/4 SG atmospheric RVs did not operate as designed (pre-existing problem). (5) No "first out" light for 1st SI. (6) Degradation of condenser vacuum. (7) Loss of PRZR steam bubble (and normal pressure control). (8) 4/5 operating CW pumps (initiator). (9) 4/5 operating CW pumps (initiator) because of severe grass intrusion at CW intake structure. (10) SG atmospheric RV failures because of pre-existing problems. (11) Spurious SI because of pre-existing design problem. (12) Failure of 12A CW pump to start as a result of circuit breakers not being fully racked in.

A.4.3 ACTION SUMMARY

Event Timeline:

```
Initiator                    Post-Accident
 10:47          11:18          11:49
_____________________________________________
   ^             ^^             ^
   U1            U2U3           R1
   |_____________||
```

Key:
U = unsafe actions
E = equipment failures
H = non-error (non-recovery) actions
R = recovery actions

UNSAFE ACTIONS AND OTHER EVENTS	
ID	Description
U1	Operators fail to control RX power (balance power and turbine) load and temperature, resulting in over-cooling then trip when power is increased to "reactor startup" trip setpoint (25%).
U2	Operators fail to terminate HPI soon enough, resulting in solid PRZR.
U3	Operators fail to control secondary pressure, resulting in SG safety valve opening, rapid cooldown, and 2nd SI.
R1	Operators manually open and close SG atmospheric dump valves to control RCS temperature and control RCS pressure through charging and letdown.

HUMAN DEPENDENCIES		
Actions	Dependence Mechanism	Description
U1, U2, U3	Training	Operators consistently fail to monitor plant condition
U1, U2, U3	Stress	Workload is very high in the control room, which leads to distraction from monitoring plant condition.

Unsafe Actions Analysis — **Salem Unit 1**

U1 EOC, Mistake Operators fail to control reactor power (balance power and turbine) load and temperature, resulting in over-cooling then trip when power is increased to reactor startup trip setpoint (25%).

Error Forcing Context

Plant Conditions	Performance Shaping Factors (PSFs)	Failures of Information Processing
Evolution/activities: 1) Continuous monitoring of condenser back pressure (and corresponding decrease in power) because of river grass interference w/circulating water (CW) traveling screens. *Operational problems:* 1) Operating at reduced power because of reductions of condenser cooling efficiency (result of river grass intrusions at the condenser's CW intake structure). 2) Grass intrusions @ CW intake structure, at least 2 per day (seasonal occurrence, severe attacks in spring and autumn - vulnerability documented for a number of years). *Unavailable: system/component:* 1) Automatic control rod control system (because of CM). *Plant functions lost:* 1) Degradation of condenser vacuum (result of CW pump loss). 2) System/components lost: operating CW pumps (initiator).	*Procedures:* 1) Guidance for rapid down power maneuvers and loss of CW pumps was weak or did not exist. As a result, atypical rate of reduction (i.e., 8% per minute) and boration was used in attempt to maintain main condenser and turbine operation despite the fact that the number of operating CW screens and pumps was below the minimum for turbine operations. 2) Insufficient guidance regarding actions required for operation with the reactor temperature below the minimum temperature for critical operations (just required recovery within 15 minutes). 3) Alarm response procedures for low vacuum conditions did not provide specific turbine trip criteria. Abnormal procedure for low vacuum did not state turbine trip setpoint. *Training:* 1) Operators failed to recognize decreasing T_{ave} immediately. 2) Operators failed to identify that a RX trip on low power-high flux condition would occur as a result of 7%-25% power increase. 3) RO responsible for rod control relatively inexperienced. *Communications:* 1) NSS does not tell rod operator that NSS withdrew rods. 2) NSS does not provide clear direction to rod operator regarding size and speed of power increase. *Supervision:* 1) SNSS left control room during down power operations to attempt to restore circulators (not procedurally directed) when his duties were to provide direction to NSS on when a reactor or turbine trip should be initiated. 2) NSS directs rod operator to leave his station to shift electrical loads when reactivity is not stable. 3) NSS does not provide rod operator with sufficient direction regarding size and speed of power increase to restore T_{ave} above minimum for criticality. *Organizational Factors:* 1) Operators not provided with adequate guidance regarding management expectations for control room activities during grass intrusions. 2) No guidance as to when operators should cease the effort to maintain plant operations and, instead, stabilize plant conditions by either turbine or reactor trip. 3) Perceived management expectations that extraordinary effort would be used to overcome grass intrusions; attention inappropriately diverted from primary systems to balance of plant (i.e., inappropriate priorities). *Stress: workload:* 1) Numerous distractions in control room during load reduction - continuing communications with CW operators and numerous assessments of plant conditions and restarts or trips of circulators (i.e., 7 trips and 3 restarts in 10 minutes before to trip) plus Unit 2 activities. Also during this period, one boron addition and 150 steps into core with CRs. 2) Rod control operator directed to leave rod control panel to shift electrical loads while reactivity not stable. 3) No additional operators obtained in anticipation of transient to compensate for rod control in manual (only 3 staff in CR at time of event - SS and 2 ROs.). 4) SNSS outside control room during power reduction attempting to start 12A CW pump.	*Situation Assessment:* 1) Expected that CW could be returned to service, focused on keeping plant at power. 2) Failed to recognize that power was still decreasing because of delayed effects of boration, unstable reactivity. 3) Failed to recognize that reactor trip would occur when power was increased to 25% ("reactor startup" setpoint). *Response Planning:* 1) Lacked plan for when to stop trying to maintain operations versus turbine or reactor trip. 2) Lacked plan for reducing power in response to condenser back pressure increases because of the severe grass intrusion. *Response Implementation:* 1) Used an atypical rate of power reduction (8% per minute). 2) Did not control power increase in response to pre-trip overcooling (NSS pulled rods then did not tell RO; because of a lack of NSS direction, RO pulled rods too many and too fast).

Notes: Grass intrusions at the CW intake structure at Salem are a seasonal phenomenon, with more severe attacks in spring and autumn which occur following diurnal tide changes. During heavy grass intrusions, high differential pressure across the CW travelling screens rapidly develops and disables the traveling screens by sacrificial failure of the shear pins that connect the screen motor to the screen gear. Once a CW traveling screen fails because of a grass intrusion, the corresponding CW pump trips off line. Losses of CW pumps or screens affect condenser vacuum. Degradation of condenser vacuum can necessitate reducing reactor power or removing the turbine from service. Operator actions to cope with a grass intrusion are governed by procedures. However, in general, the actions taken by operators are a function of the extent and rapidity of the grass intrusion (and resultant loss of circulators and condenser vacuum) and the prospects for recovery of any lost circulators. No event before to 4/7/94 required as high a rate of power reduction to compensate for the loss of CW (and minimize the increasing back pressure in the condenser).

U2 EOO, Mistake Operators fail to terminate HPI soon enough, resulting in solid PRZR — **Salem Unit 1**

Error Forcing Context

Plant Conditions	Performance Shaping Factors (PSFs)	Failures of Information Processing
Operational problems: 1) Spurious high steam flow signals because of the design which cause spurious SI. 2) Only "A" SI actuates, not "B." 3) Indications: No "first out" light for 1st SI. *Hardware failures:* 1) Not all safety equipment actuates (e.g., 2/4 MS isolation valves) on 1st SI because of a short duration of signal. Manual positioning of 10 valves required. 2) SG atmospheric RVs did not operate as designed.	*Procedures:* 1) RX trip or SI EOP used and useful in manually aligning components. 2) Correct transfer and use of SI Termination EOP. *Procedures: incomplete:* 1) No actions specified when SI train disagreement occurs. *Training:* 1) Operators did not properly monitor RCS heatup (as well as corresponding S/G pressure increase) because of decay heat and running RCPs. 2) Operators had not anticipated that the pre-trip overcooling and the post-trip heatup would fill the PRZR. No diagnosis that the post-SI sequence would result in solid PRZR. *Stress: workload:* 1) Manual alignments of components which did not automatically actuate w/ SI and concerns re: the operability of SI "B."	*Situation Assessment:* 1) Failed to monitor and recognize RCS heatup and increasing PRZR level after RT and SI. 2) Failed to understand and recognize the effect of the pre-trip cooldown, followed by heatup on the PRZR. *Response Planning:* 1) Procedures did not specify actions to be taken in response to an SI train disagreement. *Response Implementation:* 1) Took too long to terminate SI (i.e., 17 minutes to reset SI from RX trip, PRZR filled to solid or nearly solid conditions).

Notes:

1) Before reset of SI and alignment of charging and letdown, more than 30 minutes had passed, the pressurizer filled solid, and the PORVs had actuated repeatedly.

- ~ 5 minutes to realign valves which had not appropriately positioned because of SI.
- 4 minutes required to complete EOP steps, including control of AFW and isolation of MSIVs (2/4 had not closed).
- ~ 17 minutes to reset initial SI.
- ~ 17 minutes to establish pressure control with letdown and charging.

2) Salem operators took ~17 minutes to terminate SI during the 1st SI (and12 minutes for the 2nd SI) and the PRZR did become water solid. Salem's FSAR analyses include an allowance of 20 to reset SI for inadvertent actuation. However, Westinghouse recently provided information on this topic, stating that "Westinghouse has discovered that potentially non-conservative assumptions were used in the licensing analysis of [Inadvertent SI].... The PRZR shall not become water solid...within the minimum time required for the operator to identify the event and terminate the source of fluid increasing the RCS inventory. Typically, a 10 minute operator

action time has been assumed." The AIT concluded that the Westinghouse-recommended actions may need to be re-examined in light of the Salem experience.

U3 EOO, Mistake Operators fail to control secondary pressure, resulting in SG safety valve opening, rapid cooldown and second SI.

Error Forcing Context

Plant Conditions	Performance Shaping Factors (PSFs)	Failures of Information Processing
Plant functions lost: 1) Loss of PRZR steam bubble. *Safety equipment actuation:* 1) PRZR level control system tried (but failed) to maintain level by limiting letdown and increasing charging. 2) PORVs together actuated over 300 times. 3) SG atmospheric RVs (not successfully). 4) SG code safety valves.	*Procedures:* 1) No clear guidance on solid plant pressure control provided in SI Termination EOP. *Training:* 1) Operators did not recognize RCS heatup and corresponding S/G pressure increase. 2) Training: No attempt was made to control secondary pressure prior to the rapid pressure decrease that led to auto and manual actuation of SI. 3) Operators did not anticipate the effect of the lifted S/G code safety valve on the solid plant pressure (i.e., rapid pressure reduction). No diagnosis of the effect of the open safety valve on the solid plant until pressure rapidly fell. *Stress: workload:* 1) Because of his involvement in manual valve alignments, the secondary operator did not adequately monitor and maintain a stable S/G pressure. Secondary operator did not establish adequate heat removal using the atmospheric steam dumps	*Situation Assessment:* 1) Failed to recognize rising pressure in S/G. 2) Failed to anticipate rapid depressurization following S/G safety valve lifting.

R1, Recovery Operators manually open and close SG atmospheric dump valves to control RCS temperature and control RCS pressure through letdown and charging.

Error Forcing Context

Plant Conditions	Performance Shaping Factors (PSFs)	Failures of Information Processing
Plant functions lost: 1) Solid plant operation *Safety equipment actuation:* 1) PRT rupture disk fails	Notes: R1 included because of suboptimal performance. Positive operator performance: (U2) Recognized conditions requiring 2nd SI (manual as well as auto SI) and (R1) decay heat and pressure controlled by manually opening and closing S/G atmospheric dump valves and letdown and charging.	*Response Planning:* 1) No procedural guidance or plans for pressure control during solid PRZR conditions. 2) Failed to recognize or use yellow path functional recovery procedure to re-establish PRZR bubble.

A.4.4 ACCIDENT DIAGNOSIS LOG

TIME	ACCIDENT PROGRESSION and SYMPTOMS	RESPONSE
07:30	~73% power (less than full power because of marsh grass interfering with traveling screens @ CW intake structure, resulting in increase in condenser back pressure). 12A circulator out of service for water-box cleaning.	
10:16	Massive river grass intrusion @ CW intake structure begins. 13B circulating water pump emergency trips on traveling screen differential pressure (between 10:15 and 10:40 am 13A, 13B and 12B traveling screens all clog and eventually go out of service, causing corresponding CW pumps to trip off line).	
10:27	13A pump trips on high screen differential pressure.	
10:30		Power had been decreased to ~60% because of condenser back pressure (from grass interfering w/ CW traveling screens)
10:32		U1: Unit 1 operators initiate power reduction from approximately 650 MWe @ 1% minute initially (power had already been decreased from 800 MWe at this point because of condenser back pressure). Subsequently, power reduction rate was increased to 3%, 5%, then (an atypical) 8% per minute by inserting control rods and borating. (As turbine operator reduced unit load, reactor operator correspondingly reduced RX power. Initially, operators reduced turbine power ahead of RX power, resulting in power mismatch and slightly higher than normal RCS temperatures.)
10:34		Operators try to start 12A circulating water pump, but pump immediately trips as a result of the pump circuit breakers not being fully racked in.
10:39	All CW pumps except 12B have tripped.	P-8 permissive reset (reactor trip on low coolant flow in a single loop) reset (blocked) @ 36% power. 13A and 13B pumps are restarted but by 10:46 they have tripped again, leaving 12B as the only circulator in service.
10:43	Reversal of power mismatch and decreasing T_{ave}.	P-10 permissive reset @ 10% RX power (power range low setpoint RT and intermediate range RX trip and rod stop). U1: NSS directs RO at rod control panel to go to electrical distribution control panel to perform group bus transfers (shifting loads to offsite power sources). (RO gone for 3-5 minutes.) (Operators believed plant was stable, failing to recognize that RX power was still decreasing because of delayed effects of the boron addition made.)
10:44	Turbine load @ 80 MWe, RCS temp - 531°F (RCS cooled to below minimum temperature for critical operations). Low-low T_{ave} bistables trip (setpoint Tech Spec allowable value $ 541°F).	

TIME	ACCIDENT PROGRESSION and SYMPTOMS	RESPONSE
10:45	PRZR level < 17%, PRZR heaters auto-off to control level. Contraction of coolant because of low RCS temperature.	U1: NSS identifies over-cooling resulting from delayed effect of boration. NSS goes to reactor control panel and begins to withdraw control rods to raise RCS temperature - rods pulled 35 steps (from step 55 to step 90 on control rod bank D). NSS then turns control over to RO. NSS tells RO to raise power to restore plant temp. RO begins steady "pull" - 7% - 25% power. (NSS doesn't tell RO about NSS's actions, or how far or how fast to raise power.)
10:47	RX trip @ 25% - 25% power range low setpoint ("reactor startup" nuclear instrument (NI) trip). NI "intermediate range" 20% power rod stop and 25% power reactor trip did not actuate. Automatic SI on high steam flow (spurious signal resulting from pressure wave in MS lines caused by closing of turbine stop valves when turbine automatically tripped) coincident with low-low T_{ave}. All ECCS pumps start. ECCS flow paths functional, MFW regulating valves close. No "1st out" alarm for SI, SI signal received on SSPS logic channel "A" only. Not all alignments successful	
10:49		Operators enter EOP - Trip 1 procedure.
10:53		Operators manually isolate MFW. Secondary operator misses monitoring SG pressure, auto-control doesn't work because of the design. (As a result of the nature of initiating signal, SI did not successfully auto-position all necessary components, requiring operators to manually reposition affected components.)
10:58		Operators manually initiate MS isolation (only 2 of 4 MS isolation valves auto-closed at the time of auto-initiation of SI). Operators manually trip MFW pumps.
11:00		"Unusual Event" declared on the basis of "Manual or Auto ECCS actuation with discharge to vessel."
11:05		Following EOP step 36, operators reset and terminate SI. Operator notices SI logic channel "B" already reset (indicating that "B" channel had not auto-initiated) and SI logic disagreement light flashing (RP4 panel). Operators discuss whether train B should be considered inoperable. Operators begin trying to establish pressure control using letdown and charging.

TIME	ACCIDENT PROGRESSION and SYMPTOMS	RESPONSE
11:18	PRZR PORVs (PR-1 and PR-2) periodically open on high pressure (indicating PRZR was fully to solid condition). (Primary heats up because of decay heat and running RCPs while operators perform EOP steps. PRZR fills because of heatup and volume of water added by SI. SG atmospheric RVs open several times to control secondary temperature and pressure. Because of pre-existing problems with these valves, SG pressure is not controlled properly. (Concurrent with PRZR filling, SG pressure increased because of primary heatup.) T_{ave} is 552 F. SG code safety valves (11 and/or 13) open, causing rapid RCS cooldown. Because of solid PRZR conditions, rapid SG pressure decrease also results in rapid decrease in primary pressure. (This indicated that SG atmospheric RVs were not properly controlling pressure.)	Transition to EOP - 3, SI Termination. U2: Operators fail to recognize and control increasing primary temperature and pressure and PRZR level. U3: Operators fail to recognize increasing secondary pressure. Operators do not anticipate the rapid pressure reduction resulting from SG safeties opening.
11:26	2nd Auto SI - initiated by low PRZR pressure (Auto "B" only, "A" had been reset). (Low PRZR pressure setpoint >1765 psig, allowable >1755 psig). Low PRZR pressure because of RCS cooldown resulting from SG safety valves opening. Numerous PORV openings because of SI	Operators manually SI (just after auto-SI) in response to rapidly decreasing RCS pressure (when RCS pressure reached SI setpoint).
11:41		Reset and terminate 2nd SI. Operator notices SI logic in agreement (RP4 panel). Tech Spec action statement (TSAS) 3.0.3 entered as a result of two blocked auto-SI trains.
11:49	PRT rupture disc fails (as expected). (PRZR solid or nearly solid after 1st SI @ 10:47, and the 2nd SI resulted in sufficient relief of RCS to the PRT to raise level and pressure until rupture disk blew.)	Operators have no clear guidance on solid plant pressure control. They do not consider yellow path. R1: Operators control RCS temp with manual control of 3 out of 4 MS10s (SG atmospheric RVs). (Operators had difficulty with the controls for a fourth MS10 earlier.) Operators control RCS pressure through a combination of charging and letdown using the CVCS.
12:54		Because of an SG safety valve opening, difficult to control SG atmospheric RVs.
13:16		Alert declared (in order to ensure proper technical staff available). Licensee staff recognized that TSAS 3.0.3 could not be met for inoperable SI logic channels. Operators also concerned about how to properly restore the PRZR to normal pressure and level from solid RCS conditions and wanted sufficient engineering support.
13:36		The NRC entered the monitoring phase of the Normal Response Mode of the NRC Incident Response Plan. NRC Region I activated and staffed their Incident Response Center, with support provided by NRC headquarters personnel.
14:10		Technical Support Center was staffed to assist control room operators with recovery of normal RCS pressure and level control.
15:11		Operators restore PRZR bubble.
16:30		PRZR level restored to 50% (normal band), level control returned to auto. EOPs exited, IOP-6 (Hot Standby to Cold Shutdown) procedure entered.

TIME	ACCIDENT PROGRESSION and SYMPTOMS	RESPONSE
17:15		Plant cooldown initiated.
20:20		Alert terminated.
01:06		Mode 4 (Hot shutdown) entered.
11:24		Mode 5 (Cold shutdown) entered.

A.5.1 EVENT IDENTIFIER - Wolf Creek

Plant Name:	Wolf Creek
Plant Type and Vendor:	PWR/W
Event Date, Time:	09/17/94, 4:00 am
Secondary Initiator:	None
Unit Status:	Hot shutdown
Data Sources:	AEOD/S95-01 Special Report (3/95) & Wolf Creek Incident Investigation Team Report 94-04 Revision 2 (4/14/95)
Data Input By:	William J. Luckas, Brookhaven National Laboratory, (516) 344-7562 [Susan Cooper, SAIC, (302) 234-4423]

A.5.2 EVENT SUMMARY

Event Description: In September 1994, the WCNPC's Wolf Creek Generating Station had an inadvertent discharge of ≈9, 200 gals. of 350 psig reactor coolant (RC) at 235-300°F through the residual heat removal (RHR) system to the refueling water storage tank (RWST) rapidly in ≈66 seconds. Before the event, the reactor (RX) was shutdown, borated to ≈2000 ppm concentration and in the process of cooling down via one RHR train. The nonoperating RHR train was being lined up in the plant for boron recirculation because of an RHR check valve leakage from the reactor coolant system (RCS) at the same time an RHR valve was being stroked from the control room (CR). The RCS and the operating "A" RHR train loop were pressurized @ 350 psig with 2 [of 4 total] reactor coolant pumps (RCPs) operating. The pressurizer (PZR) was being filled by reducing RCS letdown as part of the cooldown. The idle "B" RHR train was being setup with an inter-system lineup to increase the train loop boron concentration from = 1200 ppm to within 50 ppm of the RCS ≈2000 ppm boron concentration by "recircing" through the 2000 ppm boron concentration RWST water.

The inadvertent discharge was initiated when an operator in the CR remotely cycled a valve while another operator out in the plant simultaneously opened a manually operated valve as part of the RHR boron recirculation activities. As indicated in the CR, the RWST high-level alarm was received while the PZR level was dropping rapidly. The blowdown was terminated after a relief crew supervising operator (SO) in the CR suggested that the CR, licensed, balance of plant (BOP) operator remotely close the RHR valve being stroke-tested.

If the event had not been quickly terminated in 66 seconds @ ≈225 psig (and decreasing), a continuing 350 psig/300°F RCS blowdown through the unpressurized portion of the RHR system would have uncovered the RCS hot leg and most likely would have introduced a two-phase, steam-water mixture into the RWST header line in 3 minutes (and possibly less). If the blowdown had lasted 6 minutes, a 90% void fraction in the RWST header line would develop and remain until the blowdown was isolated.

Event Surprises:
(1) Unrecognized design vulnerability - very severe potential problem of flashing in common ECCS header.
(2) Incompatible work activities - RHR loop boron recirculation while stroke testing certain valves
(3) Lost ≈9300 gallons of RX coolant in ≈66 seconds!
(4) Heated up ECCS supply header from RWST so as to jeopardize the ability of safety injection to function (at all).
(5) Compressed outage schedule - planned for 40 days with previous shortest of 47 days.
(6) Difficulty of operators to rely on and follow shutdown procedural guidance during LOCA and loss of RHR in this event.
(7) Poor mental model of system valves by some operators and understanding that valve stroking was not to be performed in Mode 4.

Licensee Corrective Actions:

(1) Enhance RHR operations procedure SYS EJ-120 to alert operator of potential RCS blowdown should a misalignment occur with HV-8716A or HV-8716B and BN-8717.
(2) Install a caution placard on manual valve BN-8717.
(3) Evaluate inclusion of licensee's "Incident Investigation Team Report 94-04" into operator training.
(4) Change boron concentration requirement in the RHR procedure to minimize the need to perform a boration evolution while shutting down.

ATHEANA Summary

Deviation From the "Expected" Scenario:

(1) The principal deviation from the "expected" scenario is probably how large and how quickly RCS was lost (i.e., ~9,200 gallons in ~66 seconds).
(2) Another deviation from the "expected" scenario is that the RCS loss was the result of actions performed by two, independent operators (one in the plant and the other in the control room). The "expected" scenario probably would be the result of a single action.

Key Mismatch(es):

(1) The principal mismatch was the incompatible work activities of RHR loop boron recirculation and RHR valve stroking testing. Although several factors are cited as reasons for this mismatch, the omission of the pre-requisite of being in Mode 5 or 6 (rather than Mode 4) for the stroke testing procedure certainly was a factor.
(2) The shutdown procedural guidance was apparently not a good match with the conditions the operators faced during this LOCA and loss of RHR.

Most Negative Influences:

(1) Poor mental model of system/valves by some licensed operators.
(2) Stress: workload: A compressed outage schedule was in place to accomplish all identified work in about 40 days. This schedule was several weeks shorter than previous outages at Wolf Creek. The shortest previous Wolf Creek outage ever was 47 days (completed in November 1994). Manual alignments of components which did not automatically actuate w/ SI and concerns re: the operability of SI "B."
(3) Control and outage planning heavy reliance on the control room crew to identify potential problems and ensure that plant conditions could support the planned activities.
(4) BOP operator did not take the time to perform an adequate brief, review the procedure, or review the prints prior to performing SYS EJ-120 borating RHR train "B"
(5) NSO was not adequately briefed before performing SYS EJ-120 borating RHR train "B."

Most Positive Influences:

The blowdown was terminated (in about 66 seconds) after a relief crew SO in the CR suggested that the CR, licensed, balance of plant (BOP) operator remotely close the RHR valve being stroke-tested.

Significance of Event:

Extreme or unusual conditions. None initially. Subsequently, lost ~9300 gallons of RCS (in 66 seconds).
Contributing pre-existing conditions. Isolated RHR loop boron concentration low because of leaky check valves, requiring recirculation of train "B" to RWST to raise concentration.
Misleading or wrong information. None.
Information rejected or ignored. None.
Multiple hardware failures. None.
Transitions in progress. Several activities in progress, most important of which were the stroke testing of one valve (from the control room) simultaneous with the opening of a manually operated valve (in the plant) as part of the RHR boron recirculation activities.
Similar to other events. Not known.

KEY PARAMETER STATUS	
Initial Conditions	**Accident Conditions**
Power level: 0% (subcritical) RCS temperature(°F): (via RHR in/out) 302/234°° RCS pressure: ≈350 psig RCS level: Nominal Other: PZR nearly full and filling (i.e., almost solid); boron concentration ≈2000 ppm; SGs filled up,; cold overpressure protection (COP) system armed (i.e., PZR PORVs reset to lift at ≈460 psig)	Power level: 0% (subcritical) RCS temperature (°F): ≈309 (≈+7°F due to PZR outsurge) RCS pressure: 225 psig RCS level: Lost ≈9300 gallons of reactor coolant to RWST (with overflow to radwaste hold-up tank). Other: Pressurizer low (< 17%); RCS boron concentration ≈2000 ppm; SGs filled up; at < 17% in PZR, backup heaters deenergized and RCS pressure control lost

FACILITY/PROCESS STATUS	
Initial Plant Conditions and Configurations	**Accident Conditions and Consequences**
Evolution and activities: (1) Cooling down & reducing pressure in RCS per procedure GEN-006, Rev. 27. (2) Removing RX decay heat & RCP heat for ≈4 hours by RHR Train "A." (3) Filling PZR in anticipation of going solid. (4) Testing of EDF "B" into 23th of 24 test-run. **Configuration:** (1) RHR Train "A in service to remove RX decay heat & heat input from the 2 operating RCPs. (2) 2 of 4 RCPs secured (at least 8 hours) - the other 2 help provide RX flow & RCS pressure control. (3) EDG "B" paralleled to the grid, thus the 2 secured RCPs could not be restarted (because they draw high starting current). (4) RCS/CVCS letdown flow reduced to only one 75 gpm orifice to help charging pump completely fill PZR and cool it down and keep it < 200°F for cold. (5) PZR PORVs reset to life at ≈460 psig (cold overpressure protection (COP) system armed) & positive displacement pump + 1 of 2 centrifugal charging pumps secured & their breakers locked open to help COP. (6) PZR level high alarm activated & high level indications since PZR is being filled solid and its level is above the high level alarm setpoint. (7) RHR train "B" needs to be unisolated as a backup to train "A." **Preexisting operational problem:** (1) Isolated RHR loop boron concentration low due to leaky check valves, requiring recirculation of train "B" to RWST to raise concentration. (2) Positive displacement pump and 1 of 2 centrifugal charging pumps secured & breakers locked open to help ensure cold overpressurization protection (COP). (3) Locked manual valve BN-8717 (RHR pump discharge to RWST for RHR train boron recirculation). **Initiator:** (1) Loss of RCS resulted when two valves in the RHR system were opened simultaneously.	**Automatic Response:** (1) RWST level high alarm actuated. (2) PZR level high alarm cleared. **Failures:** **Human-System Interactions** **Defeated defenses:**

A.5.3 ACTION SUMMARY

Event Timeline:

```
Pre-initiator |   Initiator        |   Post-Accident

00:01             04:10                 04:11
_____________________________________________
 ^   ^            ^                     ^
 H1  H2           U1 U2                 R1
                  |__|
```

Key:
U = unsafe actions
E = equipment failures
H = non-error (non-recovery) actions
R = recovery actions

UNSAFE ACTIONS AND OTHER EVENTS	
ID	**Description**
H1	Operator (in control room) lined up & put into service RHR train "A" & its supporting systems to continue RCS cooldown.
H2	RX operation (in control room) raises PZR level to continue RCS cooldown.
U1	NSO (out in plant) opens 8″ manual valve BN-8717* to set up for RHR train "B" recirculation to increase RHR boron concentration to within 50 ppm of RCS concentration.
U2	BOP operator (in control room), with SS's permission, strokes open HV-8716A** remotely for first time and closes same via control board pushbuttons and strokes the valve open a second time (≈30 seconds later)
R1	BOP operator recloses HV-8716A on the basis of advice of Relief SS

* BN-8717 - RHR pump discharge manual isolation valve in common 8″ discharge line to RWST for RHR train boron recirculation.

** HV-8716A - RHR Train A isolation valve in (10″) cross-over line to hot leg recirculation loops 2 and ? (remotely operated from control room)

HUMAN DEPENDENCIES		
Actions	**Dependence Mechanism**	**Description**
U1, U2	Cascading effect (because of poor communications and situation assessment)	Simultaneous and uncoordinated ex-control room actions result in loss of RCS. Opened two valves simultaneously which violated the RCS pressure boundary (i.e., initiated RHR recirculation concurrently with valve stroking).

Unsafe Actions Analysis — **Wolf Creek**

U1 EOC, Mistake NSO (out in the plant) opens 8 " manual valve BN-8717 to set up for RHR train "B" recirculation to increase RHR boron concentration to within 50 ppm of RCS' concentration.

Error Forcing Context

Plant Conditions	Performance Shaping Factors	Failures of Information Processing
Evolution and activities: 1) Removing RX decay heat and RCP heat for ≈4 hours by RHR Train "A." *Configuration:* 2 1) RHR train "B" needs to be unisolated as a backup to train "A." *Preexisting operational problem:* 1) Isolated RHR loop boron concentration low because of leaky check valves, requiring recirculation of train "B" to RWST to raise concentration. *Administrative controls:* 1) Locked manual valve BN-8717 (RHR pump discharge to RWST for RHR train boron recirculation) (i.e., requires manual set-up for isolated RHR train "B."	*Training:* 1) NSO had a poor mental model of system/valves. *Communications:* 1) NSO was not adequately briefed prior to performing SYS EJ-120 borating RHR train "B." *Stress:* 1) Time of day.	

U2 EOC, Mistake BOP operator (in control room) strokes open HV-8716A remotely twice (30 seconds between stroking) via control board pushbuttonss.

Initial Conditions: 1) RCS temperature(°F): (via RHR in/out) 302/234° 2) RCS pressure: ≈350 psign 3) RCS bsron concentration ≈2000 ppm ° *Evolution and activities:* 1) Removing RX decay heat and RCP heat for ≈4 hours by RHR Train "A." *Configuration:* 1) RHR train "B" needs to be unisolated as a backup to train "A." *Preexisting operational problem:* 1) Isolated RHR loop boron concentration low because of leaky check valves, requiring recirculation of train "B" to RWST to raise concentration. *Administrative controls:* 1) Locked manual valve BN-8717 (RHR pump discharge to RWST for RHR train boron recirculation) (i.e., requires manual set-up for isolated RHR train "B."	*Procedures:* 1) Stroke testing documentation had a pre-requisite requiring this test be done in Mode 5 or 6. It was actually performed in Mode 4 and the pre-requisite was improperly marked "N/A." *Training:* 1) BOP operator did not take the time to perform an adequate brief, review the procedure, or review the prints before performing SYS EJ-120 borating RHR train "B". 2) Poor mental model of system/valves by some licensed operators. *Supervision:* 1) "On-shift SO did not exercise proper command and control techniques to maintain full awareness of plant conditions." SO authorized the simultaneous performance of two incompatible work activities. *Organizational Factors:* 1) Control and outage planning heavy reliance on the control room crew to identify potential problems and ensure that plant conditions could support the planned activities. 2) Operators failed to plan and appropriately control work activities in that two incompatible activities were allowed to be performed simulataneously. *Stress:* 1) A compressed outage schedule was in place to accomplish all identifed work in about 40 days. This schedule was several weeks shorter than previous outages at Wolf Creek. The shortest previous Wolf Creek outage ever was 47 days (completed in November 1994). Manual alignments of components which did not automatically actuate w/ SI and concerns re: the operability of SI "B." 2) Time of day	*Situation Assessment:* 1) Failed to monitor and recognize RCS heatup and increasing PRZR level after RT and SI.

A.5.4 ACCIDENT DIAGNOSIS LOG

Time	Accident Progression and Symptoms	RESPONSE
20:00	Cold Overpresure Protection (COP) system armed; PDP & 1 of 2 CCPs secured and their motor breakers open.	
21:25		SS held discussions with maintenance staff involved with retest of HV-8716A which includes valve stroking with concurrent packing adjustment.
00:01	H1: Operator (in control room) lines up and puts in service "A" RHR train and its supporting systems to continue RCS cooldown.	
	H2: RX operator (in control room) controlling CVCS to slowly increase PZR level in preparation for going solid.	
03:00		Again, SS held discussions with maintenance staff involved with retest of HV-8716A. SS also granted permission to adjust packing.
04:10	**U1**: NSO slowly starts to open 8" manual valve BN-8717 to manually set up for RHR train "B" recirculation to match RCS boron concentration.	
	U2: BOP operator strokes open HV-8716A, remotely for the first time.	
04:10 : 30	**U2**: BOP operator strokes open HV-87167A, remotely for second time (30 seconds after first)	

A.6.1 EVENT IDENTIFIER - Davis-Besse

Plant Name:	Davis-Besse
Plant Type and Vendor:	PWR/B&W
Event Date, Time:	06/09/85, 1:35 am
Event Type:	Loss of Main and Auxiliary Feedwater
Secondary Initiator:	None
Unit Status:	Full-power
Data Sources:	NUREG-1154, July 1985
Data Input By:	John Wreathall, Wreathall & Co., (614) 791-9264 [Susan Cooper, SAIC, (302) 234-4423]

A.6.2 EVENT SUMMARY

Event Description: In June 1985, Davis-Besse, following a history of main feedwater pump (MFP) spurious trips, was operating with 1 of 2 MFPs in manual control. The other MFP tripped, causing a reactor trip. The operator, anticipating the Steam Generator (SG) low-level signal to initiate auxiliary feedwater (AFW) automatically, attempted to use manually the Steam Feedwater Rupture Control System (SFRCS) pushbuttons to initiate AFW. However, he inadvertently pressed the pushbuttons that isolate AFW from the SGs. After a brief delay, the operators reset the SFRCS and initiated AFW. Because of two separate common cause failures, the AFW system failed to provide feedwater. Equipment operators (EOs) were dispatched to recover operation of the AFW pumps and valves and to initiate the manual startup (SU) feedwater system. However, the SGs reached "dryout" conditions, thus meeting the requirement to begin RCS feed-and-bleed cooling. The operators delayed feed-and-bleed cooling in the belief that SG feed and secondary inventory for RCS heat removal were about to be recovered, which it was.

Event Surprises: None.

Licensee Corrective Actions: None.

ATHEANA Summary

Deviation From the "Expected" Scenario:

1) Multiple common-mode failures of the AFW system was a significant deviation from the operators' expectations of equipment performance in their scenario and delayed their response.
2) The operator's attempt to use, and the lock-out feature of, the SFRCS that prevented automatic initiation of the AFW system was a deviation from the expected scenario.

Key Mismatch(es):

1) The time required to restore the failed AFW system compared with the operators' expectations of restoring the system was a key mismatch.
2) The operators' confidence in restoring AFW compared with the procedural guidance of when to initiate feed-and-bleed operations mismatched.

Most Negative Influences:

1) For the delay of feed-and-bleed, the operators perception that the consequences of feed-and-bleed were very drastic and their confidence that some sort of feedwater would be recovered dominated.
2) Various common cause hardware failures, including those that resulted in the loss of all feedwater, occurred.
3) For inadvertent isolation of AFW, human engineering of the panel (i.e., location and layout), lack of training and experience, and perhaps, the time of day were important.

Most Positive Influences:

1) Timely ex-control actions of the equipment operators saved the plant from damage.

Significance of Event:
Extreme or unusual conditions. None initially. Subsequently, steam generators reach "dryout" conditions and feed-and-bleed criteria.
Contributing pre-existing conditions. Multiple conditions that probably contributed to this event, (e.g., recent history of spurious feedwater pump trips, feedwater pump #2 in manual control, torque switches on AFW isolation valves incorrectly set, and SPDS was inoperative in the control room).
Misleading or wrong information. PORV position indicated that valve was shut (when it was actually stuck open).
Information rejected or ignored. Sonic signals indicating open PORV. (Block valve was closed as a precaution despite the fact that operators did not understand that the PORV was open.)
Multiple hardware failures. AFW system (once because of operator error, twice because of separate common cause failures), PORV stuck open, control room HVAC tripped into emergency mode, main turbine did not go to turning gear.
Transitions in progress. None.
Similar to other events. Recent experience with spurious MFW pump trips at power. MFW pump #2 in manual control for this reason.

KEY PARAMETER STATUS	
Initial Conditions	**Accident Conditions**
Power level: 90% RCS temperature (°F): 582 RCS pressure: 2170 psig RCS level: Nominal Other: PZR level - 200," SG level - normal	Power level: 0% RCS temperature (°F): 592 RCS pressure: 2440 psig RCS level: Other: PRZ level - 76-300", SG level - 8". Minimal inventory loss via PRZ PORV.

FACILITY/PROCESS STATUS	
Initial Plant Conditions and Configurations	**Accident Plant Conditions and Consequences**
Configuration: Normal **Preexisting operational problem:** Repeated recent history of spurious MFP trips at power (1) MOV torque switches incorrectly set (unknown to plant) (2) Main feedwater pump #2 in manual control. (3) Positive displacement pump and 1 of 2 centrifugal charging pumps secured & their breakers locked open to help ensure COP. (4) One source range NI channel inoperable. (5) PZR high level alarm & indications were unavailable, since the PRZ is being filled solid and its level is above the high alarm setpoint. (6) SPDS inoperative in control room. **Initiator:** Loss of main and auxiliary feedwater resulted from an combination of human and hardware (including common cause) failures.	**Automatic Response:** (1) RT because of a loss of main feedwater. **Failures:** (1) AFW turbine pumps (2) tripped; would not reset. AFWTP trips caused by flashing of saturated water in turbine nozzles. (2) AFW isolation valves (2) failed closed. AFW isolation valves – bypass contacts on torque switches mis-set. (3) PZR PORV stuck open on 3rd opening. (4) CR HVAC spuriously tripped to emergency mode. (5) Main turbine did not go to turning gear. **Human-System Interactions** **Latent failures:** (1) AFW isolation valves with incorrectly set torque switches (design unsafe act) **"Aggravating actions":** (1) Operator inadvertently caused isolation of both SGs – slip **"Things left undone":** (2) Intentional failure to initiate feed-and-bleed

A.6.3 ACTION SUMMARY

Event Timeline:

Pre-initiator |	Initiator |	Post-Accident			
	01:35	01:41	01:42	01:51	01:53
^	^	^	^	^^^^	^^
U1	E1	U2	R1, R2	U3, R3, E3, & E4	R4, R5

Key:
U = unsafe actions
E = equipment failures
H = non-error (non-recovery) actions
R = recovery actions

UNSAFE ACTIONS AND OTHER EVENTS	
ID	**Description**
U1	Maintenance personnel miscalibrated torque switches on AFW isolation (isol.) valves.
E1	MFW pump "1" trips → RX & turbine trip on high RCS pressure.
U2	Operator inadvertently selects wrong buttons on SFRCS (low SG pressure) in anticipation of automatic low SG level → isolates both.
R1	Shift supervisor (SS) resets SFRCS & correctly presses low SG level buttons.
E2	AFW isolation valves fail to open.
R2	EOs dispatched to equipment areas to recover: AFW pumps, SU feedwater pump, AFW isol. Valves.
E3	SG atmospheric dump valve sticks open.
E4	PZR PORV sticks open.
U3	Operators decline to implement "feed-and-bleed" despite (1) procedures, and (2) management instructions.
R4	AFW train 2 has significant flow.
R5	AFW train 1 has significant flow.

HUMAN DEPENDENCIES		
Actions	**Dependence Mechanism**	**Description**

Unsafe Actions Analysis		Davis-Beese
U1 EOC, Unknown maintenance personnel miscalculated torque switches on AFW isolation (isol.)		
Error Forcing Context		
Plant Conditions	**Performance Shaping Factors**	**Failures of Information Processing**
Not Known		
U2 EOC, Slip Operator inadvertently selects wrong buttons on SFRCS		
Error Forcing Context		
Plant Conditions	**Performance Shaping Factors**	**Failures of Information Processing**
Notes: NUREG-1154 does not discuss any causes of this event.	*Training:* 1) Operation of the SFRCS often not covered in training. 2) Manual anticipation of automatic operation "common." *Human-System Interface:* 1) Poor location of panel. 2) Confusing layout of switches. *Stress:* 1) Time of day. *Other:* 1) Operator had never used SFRCS before.	*Response Implementation:* - Operator inadvertently selected wrong pushbuttons on a confusingly designed and poorly located control panel.
Notes:		
U3 EOO Correct violation Operators decline to implement "feed-and-bleed"		
Error Forcing Context		
Plant Conditions	**Performance Shaping Factors**	**Failures of Information Processing**
Three consequence of feed-and-bleed operations would have been 1) to breach one defined raiological barrier (RCS boundary); 2) to create operational difficulties and uncertainties in reaching cold shutdown; and 3) delayed restart to clean up contaminated areas.	*Communications:* 1) Shift supervisor was in phone communications with the operations superintendent when SG s were "drying out"; potentially delayed response. *Human-System Interface:* 1) SG level indication not adequate to determine if feed-and-bleed criteria met (8″ indicated on a scale of 0-250″). 2) SPDS out of service (could have provided backup indication of SG level). *Stress:* 1) Fee-and-bleed judged to be "pretty drastic."	*Response Planning:* - Operator deliberately elected to delay implementing feed-and-bleed in the expectation that feed flow would be available shortly.
Notes: The delay in implementing feed-and-bleed instructions once the criterion of dryout (8″) had been met was only 3-5 minutes. The operator had knowledge of the actions to restore SG cooling.		

A.6.4 ACCIDENT DIAGNOSIS LOG

Time	Accident Progression and Symptoms	Response
01:35	MFW pump 1 trips; reactor and turbine trip shortly thereafter	Operators attempt to increase feedwater flow using Pump 2 but insufficient to prevent trip.
01:36	MSIVs closed	
01:40	MFW pump 2 terminates feeding because of low steam pressure	
01:41	Falling SG water levels noted by secondary-side operator (< 27″)	**U1:** In attempting to anticipate the automatic initiation of AFW, operator inadvertently isolates SGs.
01:42		**R1:** Shift supervisor resets SFRCS, attempts to start AFW. Multiple hardware failures cause failure of both trains of AFW.
01:42	Failure of AFW system	**R2:** Operators dispatched to manually start SUFP and recover AFW equipment.
01:48	Both SGs meet "dried out" criterion as defined in EOPs (pressure < 960 psig)	
01:51	RCS pressure at 2425 psig and falling (Pressurizer PORV stuck open - **E3 & E4**)	**R3:** Operator does not diagnose PORV stuck open ("demand" position, not actual position indicated; overlooks sonic signals), but closes PORV block valve as a precaution (also PZR spray valve).
01:51	SG levels and pressure (<8″ , <960 psig) meet feed-and-bleed criterion	**U3:** Operators postpone feed-and-bleed instruction in procedure.
01:51	SUFP operating, feeding SG #1	
01:53	AFW train 2 providing "significant flow" - **R3**	
01:54	AFW train 1 providing "significant flow" - **R4**	
02:04	Plant stable	

APPENDIX B
ATHEANA EXAMPLE -
DEGRADATION OF SECONDARY COOLING

This appendix illustrates the use of the ATHEANA process to investigate the potential for operator actions that would result in the inappropriate reduction of secondary cooling in a pressurized water reactor (PWR). More specifically, it is an illustration of the use of ATHEANA to identify and quantify those circumstances (contexts) that may induce human actions involving the inappropriate degradation or nonrestoration of secondary cooling during an event where secondary cooling has been initially disrupted and needs to be properly restored and maintained to provide adequate core cooling.

This is a plant-specific example, as all fruitful examinations of context must be. However, the plant analyzed is a composite PWR, not exactly matching any particular plant. The example is realistic in that all specific design, procedures, training and operating and maintenance practice information used in the analysis have been observed in real plants. As a result, this example provides a basis for licensees desiring to investigate a similar issue at their plant.

The example follows the steps discussed in the ATHEANA process in Section 9 of this document.

B.1 Step 1: Define and Interpret the Issue

This analysis identifies the possible conditions that might induce nonrestoration, shutting off, or at least, inappropriate reduction of secondary cooling in a PWR in response to an event involving an initial loss or serious degradation of steam generator secondary cooling flow during full-power plant operation. Throttling of secondary flow is part of the normal response after reestablishment of secondary cooling following a reactor trip in response to such an event. However, industry experience includes events where premature or excessive throttling of secondary cooling has occurred. In light of this experience, the purpose of this analysis is to identify those circumstances (contexts) that may induce human actions involving the inappropriate degradation or nonrestoration of secondary cooling during such an event. The results of the analysis are to be used to make any improvements (procedure changes, training changes, human/machine interface changes...) that would lessen the likelihood of operators inappropriately reducing secondary cooling during an event of this type.

B.2 Step 2: Define the Scope of the Analysis

Based on the description of the issue provided in Step 1, a review of representative initiators from Table 9.1, a direct internal plant transient, specifically loss of main feedwater (MFW) while at full power, was selected as the most relevant type of initiating event to use as the basis for examining this issue. The following reasons are offered for this selection.

First, loss-of-coolant accidents (LOCAs) involving the reactor coolant system (RCS), except for the smaller breaks, do not need nor are sensitive to the success of secondary cooling in order to achieve successful mitigation of the event. This is shown, for example, by the large LOCA event tree reproduced here from this plant's PRA (see Figure B.1). It shows no need for secondary cooling to achieve successful mitigation of the event. For the breaks of smaller sizes, the lack of proper

secondary cooling does contribute to how the scenario proceeds, but it is generally not as important as early RCS injection in determining the outcome of the event (safe or core damage). In addition, while the small LOCA and loss of main feedwater scenarios have similar needs for secondary cooling, the expected frequency of a small LOCA is two to three orders of magnitude less than that for a loss of main feedwater event, making the latter event much more likely to be experienced and therefore of more interest.

Second, virtually all transients (e.g., turbine trip) at this plant involve a concurrent initial loss of the normal feedwater anyway since the main feed regulating valves close on low T_{avg} (554°F) which is expected to occur in most events involving reactor trip. While other transient initiators with a concurrent loss of main feed may add complexity to the event, the complexities will be considered in this analysis to the extent that they do not represent other specifically analyzed initiators in this plant's PRA. For example, even though loss of instrument air is a form of transient that could contribute to the loss of main feed and add other complexities to the scenario, loss of instrument air is explicitly treated as another type of initiator in the PRA and will be considered outside the scope of this illustrative analysis.

Third, the loss of main feedwater event chosen has the characteristic that the need to reestablish secondary cooling is paramount. In this type of initiating event, human actions involving the disruption or prevention of secondary cooling could have serious consequences and even cause damage to the core if this and alternative means of cooling the core (e.g., feed and bleed) are not established. Based on these observations, the loss of main feedwater scenario is chosen as the most relevant form of accident for which to examine the defined issue.

The plant's PRA already covers the loss of secondary cooling (including the loss of auxiliary feedwater) due primarily to equipment failures. This loss is shown as contributing to core damage sequences 4 and 5, as well as the outcome to 6 [depending on the steam-driven auxiliary feedwater (AFW) train] in Figure B.2, for the loss of main feedwater initiator in the PRA. This ATHEANA analysis examines the potential contexts and the likelihood of a loss or degradation of secondary cooling due to operator actions not already covered in the PRA. Hence, the operator actions of interest contribute to those same sequences in ways not included in the current PRA.

Since this is a specific issue to be analyzed, there is no requirement to consider additional limitations of scope in this step beyond limiting the analysis to the loss of main feedwater initiator. Also, since this example is analyzing a specific issue, there is no need to prioritize among numerous issues or analyses that might be performed.

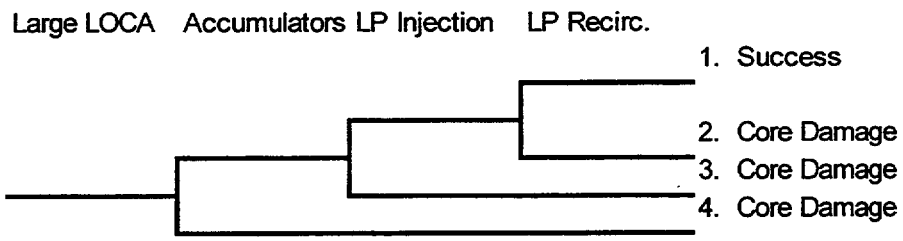


Figure B.1 Large LOCA Event Tree

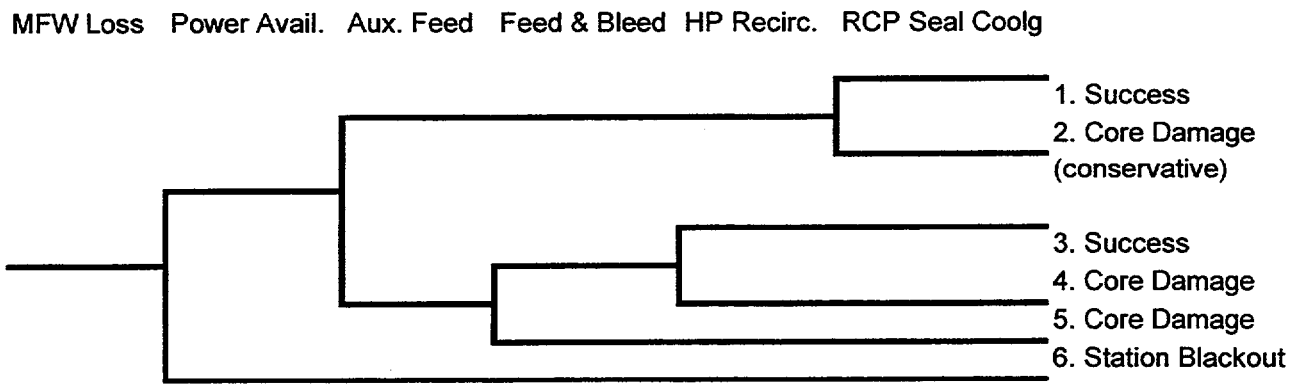


Figure B.2 Loss of Main Feedwater Event Tree

B.3 Step 3: Describe the Base Case Scenario

B.3.1 Introduction

This step of the analysis process defines a base case scenario for the loss of main feedwater event from which to develop other scenario contexts that may challenge the operating crew in ways that may be "error forcing." Ideally, the base case scenario has the characteristics shown in the first row of Table B.1; i.e., the scenario description represents a consensus of the expected plant response by most operators, it is well defined operationally, there are well-defined physics descriptions and adequate documentation of the plant response, and the scenario is realistic. As will be explained below, the base case scenario for this analysis has the characteristics shown in the second row of Table B.1.

Table B.1 Characteristics of Base Case Scenario

Base Case	Consensus Operator Model	Well-Defined Operationally	Well-Defined Physics	Well-Documented	Realistic
Ideal	Exists	Yes	Yes	Yes	Yes
Loss of main feed scenario	Based on what is "expected" by most operators as described in the text	Yes, in accordance with consensus operator model	Will start with a final safety analysis report (FSAR) version (called reference scenario)	Will start with a FSAR version (called reference scenario)	Yes, by modifying the FSAR version to make it more like the consensus operator model

The discussion starts with a well-documented reference scenario (from the FSAR) for the loss of main feed event and develops a "base case" scenario that is more in line with the expected plant and operator response for a loss of main feedwater event while the plant is operating at full power. The expected plant and operator response represents that which is well within the operators' training background and coincides with their limited experience of responding to an actual event at this plant. Purposely, no equipment failures or other complexities are considered in the expected scenario (the "base case" scenario) since these will be considered later as possible "deviations" from the base case scenario. Hence, this step provides a base case "signature" for a loss of main feed event from which additional complexities are later proposed that may make the operator response to the event "error-forcing" in a way described by the issue as summarized in Step 1.

B.3.2 Use of a Reference Case Scenario (from FSAR)

The base case loss or degradation of main feedwater scenario while the plant is at power is derived from the plant's FSAR Chapter 14, safety analysis, loss of normal feedwater accident analysis. This accident analysis serves as what will be referred to as the "reference scenario" from which the base

case scenario is derived. Operations staff receive periodic training on this type of event and thus a "knowledge of the event" and expectations of how the plant responds to such an event have been formulated in the minds of the plant's operators.

Based on the FSAR reference scenario, the loss of main feedwater while at power is an anticipated abnormal event which should not pose a threat of offsite radiation consequences. As stated in the FSAR, *a loss of normal feedwater results in a reduction in capability of the secondary system to remove the heat generated in the reactor core.* The FSAR cites the following features that protect against the loss of normal feedwater:

- *Reactor trip on low-low water level in either steam generator*
- *Reactor trip on steam flow; feedwater mismatch coincident with low water level in either steam generator*
- *Two motor-driven and one turbine-driven auxiliary feedwater pumps that start automatically on low-low level in either steam generator* [among other signals]

There are a number of conservative assumptions included in the FSAR analysis which apply to the reference scenario that is used to develop a description of the base case (expected) scenario. Among these are the following:

- the initial steam generator water levels are minimized
- initial plant power is 102%
- use of a heat transfer coefficient in the steam generators assuming natural (not forced) circulation
- use of a conservative heat generation rate
- credit for only one motor-driven auxiliary feedwater pump to only one of the two steam generators
- fouled steam generator tubes
- coincident loss of offsite power so that natural circulation flow exists in the reactor coolant system
- no credit for the nonsafety steam generator pressure control features.

These conservative assumptions tend to maximize the "effect" of the scenario and collectively result in an exaggeration of what is normally expected during a loss of main feedwater. Hence, the FSAR

analysis as the reference scenario is not fully consistent with the *base case* and more realistic plant response. Nevertheless, the FSAR analysis can be used to form the base case response.

The FSAR describes the expected sequence of events as follows:

> *Following the reactor and turbine trip from full load, the water level in the steam generators will fall due to the reduction of steam generator void fraction and because steam flow through the safety valves continues to dissipate the stored and generated heat ...following the initiation of the low-low level trip the auxiliary feedwater pump is automatically started reducing the rate of water level decrease. Sufficient heat transfer is available to dissipate core residual heat without water relief from the primary system relief or safety valves. If the auxiliary feed delivered is greater than that of one motor driven pump...the result will be a steam generator minimum water level higher than shown... .*

The FSAR concludes:

> *The loss of normal feedwater does not result in any adverse condition in the core, because it does not result in water relief from the pressurizer relief or safety valves, nor does it result in uncovering the tube sheets of the steam generator being supplied with water.*

The FSAR provides figures for the reference case which are duplicated here and where the following points are clearly presented:

- Figure B.3 shows that the average coolant temperature within the core region (T_{avg}) quickly drops upon reactor scram, then rises due to the initial mismatch between the heat generation and the degradation of heat removal because of the loss of main feedwater. Upon the initiation of the AFW system and as it provides sufficient water to the steam generator, the core coolant temperature then gradually falls again as reactor decay power continues to decrease and heat sink capability is fully restored via at least one steam generator.

- Figure B.4 shows the pressurizer liquid volume, which shrinks, expands, and then gradually decreases, following a trace roughly coincident with the T_{avg} plot above. Since the mass of the RCS is not changing, pressurizer level is a direct function of T_{avg} (i.e., RCS volume is proportional to T_{avg}).

- Figure B.5 shows the steam generator water level response within the fed steam generator, which falls due to steam flow/feed flow mismatch until the AFW system (AFWS) initiates and restores the water level.

B.3.3 Base Case Scenario

The base case scenario, largely on the basis of the "expected" consensus opinion of the operators (i.e., a consensus operator model), differs from the above reference scenario in that (a) all AFWS pumps successfully respond, (b) feeding to both steam generators occurs, (c) nonsafety RCS and

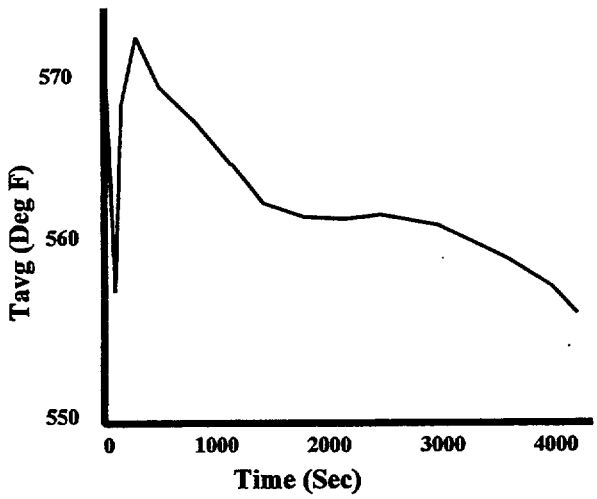


Figure B.3 T_{avg} During Loss of Main Feed.

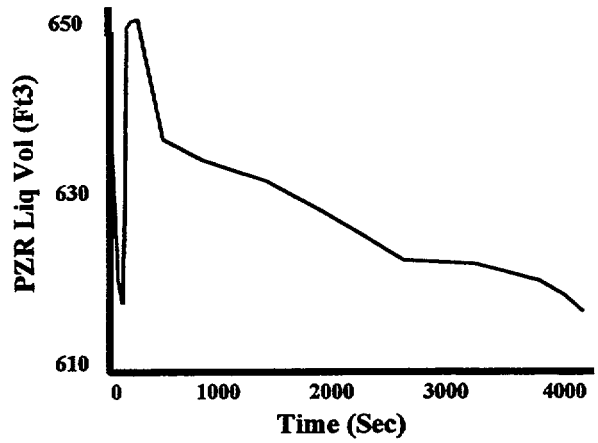


Figure B.4 Presurizer Volume During Loss of Main Feed.

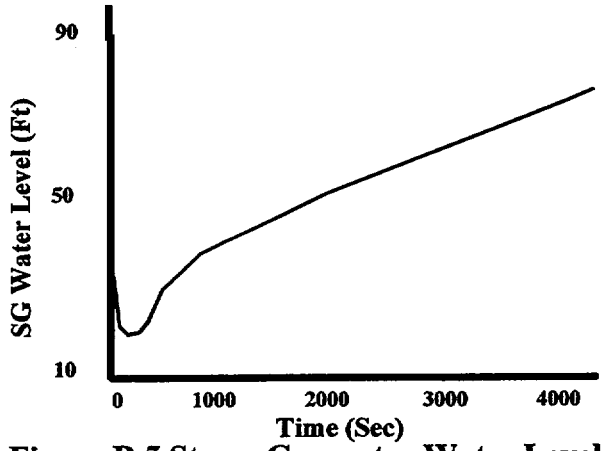


Figure B.5 Steam Generator Water Level During Loss of Main Feed.

steam generator control systems also function, and (d) the conservative assumptions used in the reference scenario do not exist. These are the primary features of the operators' consensus opinion of what is expected to occur in this type of scenario. As a result, the effects of the event would not be quite as severe for the base case scenario, which is defined to have the features of the consensus operator model. In particular, both steam generator water level responses would be similar since both steam generators are assumed to be fed. In addition, the changes in T_{avg} and pressurizer level may be slightly different due to operation of nonsafety equipment such as the steam dumps and pressurizer heaters. Nevertheless, the base case plant response can be approximated by that illustrated by the three figures above. These figures, along with other figures presented below, are considered sufficient to generally describe the base case scenario.

Based on the above reference case from the FSAR analysis, knowledge of the emergency operating procedures (EOPs) (discussed later), expert judgment, and with no equipment faults or inappropriate operator actions, the following is presented as a summary of the "base case" and realistic plant response to a loss of main feedwater type of initiating event. This summary and the accompanying representations of the key parameter indications observable to the operators and shown in Figures B.6 through B.12 provide the expected "signature" of the event and what the operators are likely to expect and respond to as the scenario progresses, assuming there are no additional complexities (i.e., deviations).

- Initial Condition: The plant is operating at full power when a loss of normal feedwater occurs as a result of valve malfunctions, feedwater control anomalies, or similar faults. Indications or alarms of the loss of flow condition are the first cues to the operators.

- The rapid drop in steam generator levels and the steam-feed flow mismatch quickly cause a reactor trip.

- Sufficient low levels in the steam generators auto start all available auxiliary feedwater pumps if operators have not already manually started the system.

- Following plant trip until the plant is stabilized, the expected responses occur as highlighted by the following:

  (1) Reactor power decreases nominally following the reactor trip, as evidenced by the typical indications and power (flux) time history shown in Figure B.6.

  (2) The turbine trips and the generator load drops as evidenced by the typical indications and turbine pressure time history as shown in Figure B.7.

  (3) All electric buses (key support system) continue to operate (including required bus transfers) and appear normal based on breakers indicating "closed," available bus voltages and related indications that are nominal; and expected operating loads that are operating as evidenced by current, flow, and similar readings.

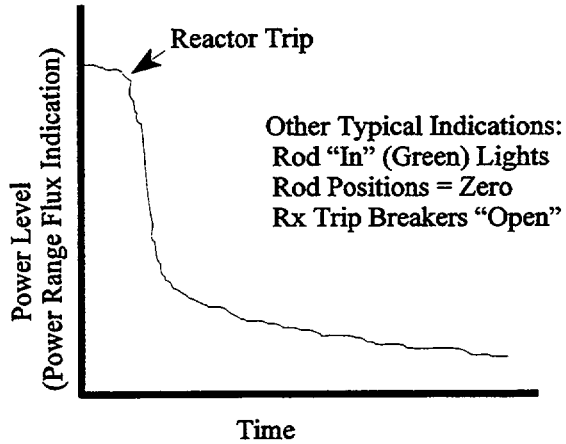


Figure B.6 Power Level vs. Time

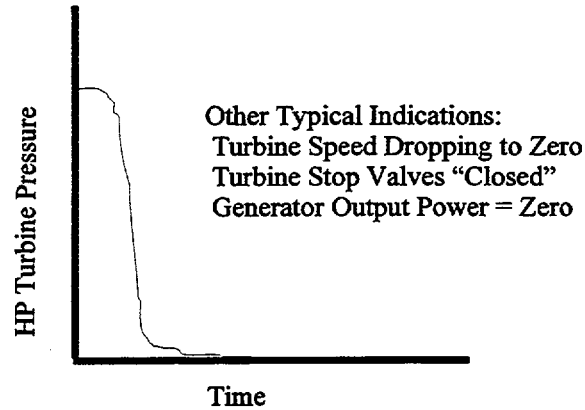


Figure B.7 Turbine Pressure vs. Time

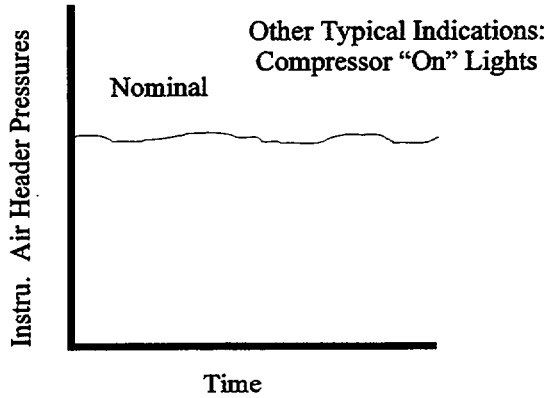


Figure B.8 Instrument Air Pressure vs. Time

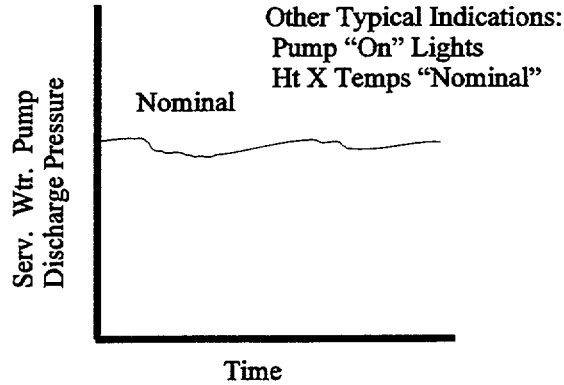


Figure B.9 Service Water Pressure vs. Time

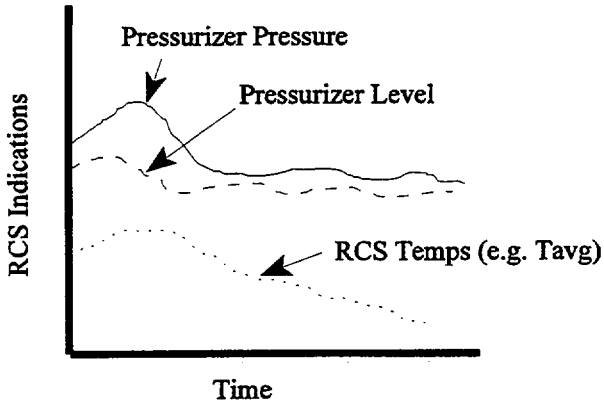


Figure B.10 RCS Conditions vs. Time

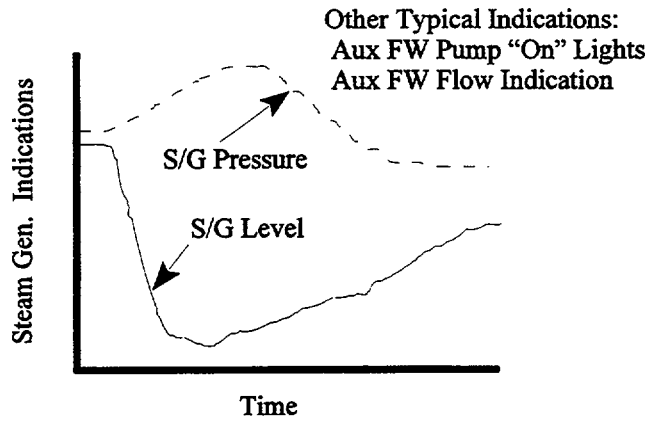


Figure B.11 Steam Generator Status vs. Time

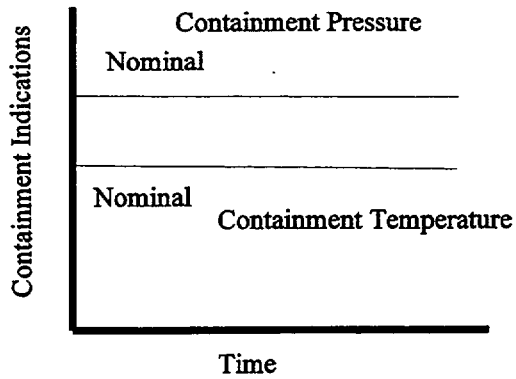


Figure B.12 Containment Conditions vs. Time

(4) Instrument air, a support system, is available, as evidenced by no change in header pressures over time as shown in Figure B.8 and appropriate compressor "on" lights.

(5) As another set of key support systems, component cooling water (CCW) and service water (SW) pump lights are "on," pump discharge pressures remain nominal over time as illustrated in Figure B.9, and service water load temperatures are nominal. Note that some momentary disturbances in the pressures and flow rate may be evident if some loads are isolated or other realignments occur. These disturbances are momentary.

(6) Key indications for the status of the RCS go through time history responses typical of that shown in Figure B.10. These are indicative of a rapid loss of heat sink (as feedwater is lost to the steam generators but is eventually recovered with auxiliary feedwater) along with the effects of reduced power (when the reactor trips) and normal operation of chemical volume control system (CVCS) charging or letdown and pressurizer heaters or sprays as they compensate for disturbances in RCS conditions. Neither pilot-operated relief valve or safety relief valve (PORV/SRV) demands occur nor is safety injection actuated in this event. Key indications such as pressurizer pressure, level, and RCS temperatures (T_{hot}, T_{cold}, T_{avg}...) rise as the RCS heats up and swells due to the degrading heat sink. Then they are restored and maintained within normal limits as the reactor power decreases, heat sink is eventually restored with auxiliary feedwater, and the charging or letdown and pressurizer spray or heater systems function normally. Pressurizer pressure does not reach PORV set points or drop to a safety injection limit. Similarly, pressurizer level does not reach high or "solid" condition or drop to that requiring safety injection. RCS temperatures do not reach extreme high or low levels requiring quick changes to reactor coolant pump (RCP) pump operation or other significant human actions.

(7) Steam generator levels drop dramatically at first due to the loss of feedwater, but with auto (or manual) start of auxiliary feedwater, levels soon show signs of restoring as shown in Figure B.11. Steam generator pressures rise at first as RCS heat continues to be dumped to the degrading steam generator, but with reactor trip and recovering steam generator levels, pressure is restored and ultimately controlled via the steam generator blowdown system. Main steam safety valves (MSSVs) are not actuated unless there is a corresponding and sudden main steam isolation. Auxiliary feedwater pump indications and valve alignment lights indicate flow into the steam generators. As the steam generator heat sinks are recovered, auxiliary feedwater is throttled down by the operator and if not needed, the turbine pump is shut down and placed in "pull-to-lock."

(8) Nominal containment conditions remain unchanged, as represented in Figure B.12.

(9) No radiation indicators or alarms are present.

(10) No other adverse indications or alarms such as ventilation problems are present.

- With no developing complexities (i.e., no "deviations" from the base case response to a loss of main feedwater event), an early focus by the operators is on recovering and then controlling steam generator pressures and levels within prescribed limits to restore and maintain proper heat sink. The turbine-driven auxiliary feedwater pump is shut down and put in pull-to-lock to avoid overcooling while flow from the other auxiliary feedwater pumps is throttled as necessary. Steam dump is performed to the condenser (most likely still available) or using, for instance, atmospheric dump valves to control steam generator pressure and eventual depressurization.

- Cooldown of the plant and shutdown of unnecessary equipment commences, achieving either a stable hot shutdown status or proceeding to cold shutdown if required.

Note that in the base case scenario, operator actions primarily involve: (a) verification of the above automatic equipment responses and that no additional failures of equipment have occurred via available indications, (b) controlling steam generator levels and pressures, including throttling of auxiliary feedwater flow so as to not overfill the steam generators, and (c) cooling down the plant and shutting down unnecessary equipment as required.

B.4 Step 4: Define Human Failure Events (HFEs) and Unsafe Actions (UAs)

Based on the issue as defined in Step 1, functional failure modes 2, 3, and 5 from Table 9.6 are the most relevant given the desired automatic recovery of secondary cooling via AFWS and the use of steam dumps and other equipment. From Table 9.7, corresponding HFEs associated with these functional failure modes involve equipment being inappropriately terminated, isolated, or controlled, as well as failing to be backed up upon automatic failure, among other similar examples. Based on these examples of HFEs, two general types of HFEs are defined here that are relevant to the issue as defined in Step 1. These are:

HFE 1: Operator actions that involve the inappropriate termination/isolation/realignment or at least severe reduction of secondary cooling via the steam generators because it is envisioned as the appropriate response (even though it is actually inappropriate). Of interest are those actions that lead to degradation of secondary cooling and hence additional challenges for the safe recovery from the loss of main feedwater event. Note that such actions could, for instance, involve a number of different specific UAs such as shutting down the AFWS pumps, severely throttling auxiliary feedwater flow via operation of the flow control valves, restricting steam generator pressure control and subsequent cooldown, or other specific unsafe actions that result in operator-caused insufficient secondary cooling. [An error of commission (EOC)].

HFE 2: Operator failure to back up the failed or lost function of secondary cooling (such as that due to multiple AFWS equipment failures) when backup or restoration is required. Other problems competing for operator attention could be, for instance, the cause for such inaction. Illustrative of this HFE is the unsafe action of not attempting to manually restart an AFWS train. [An error of omission (EOO)].

In a PRA context, either HFE, if it persists, is another way of causing AFWS failure in the sequences shown in Figure B.2, and could therefore result in the need for feed-and-bleed cooling or even challenge the scenario to the point of potentially causing core damage due to the loss of heat removal and the subsequent heatup of the RCS.

Another form of HFE that instead leads to overfill of the steam generators or some other form of overcooling could also be of interest. However, that HFE is not the subject of the issue as defined in Step 1; thus it is not included here.

B.5 Step 5: Identify Potential Vulnerabilities in the Operators' Knowledge Base

This step is the first involving the identification of deviations from the base case scenario that may introduce contexts in which the relevant HFEs are potentially likely. Consideration of characteristics of the scenario, formal rules and procedures, informal rules, operator tendencies and biases, potential procedural difficulties, and potential timing and workload issues are among the factors involved in identifying such deviations. This step reviews potential vulnerabilities that may make the HFEs likely. As such, this step provides insights into the traits of the deviations that should be included in the next step which explicitly develops the possible scenario deviations.

B.5.1 Potential Vulnerabilities in Operator Expectations for the Scenario

Examination of Table 9.10, which addresses event types and related potential operator vulnerabilities, results in the following observations relevant to this analysis.

- The loss of main feedwater event fits a class of events that are anticipated several times during the life of the plant and for which operators at this plant are trained relatively frequently compared with other abnormal and accident events. As such, their training for such an event as well as a few actual plant transients of this type have provided an "expectation" as to what such a scenario "looks like" and the expected plant equipment and indicator responses.

- The base case scenario, i.e., without complications, has been included in training and actually been experienced in a real event by a few of the operators. Some complications have also been included in training, particularly those included in the FSAR, such as scenarios involving partial losses of auxiliary feedwater.

Based on the above observations, it should be the focus of the deviation analysis (which follows later in Step 6) to identify scenario complexities involving other (nontrained or infrequently trained) equipment failures, subtle dependent failures, or other reasons for unexpected abnormalities that make the event different from operators' conditioned expectations and might alter the operator response in a way that results in the HFEs of interest. A scenario(s) with such mismatches between operators' expectations and the actual events represents a vulnerability that may induce typically expected actions by the operators that may be wrong or at least "not ideal" for the actual situation.

B.5.2 Time Frames of Interest

As a further insight into the potential for the HFEs of interest to occur, four time periods of interest to the scenario can be identified relative to the potential for operator influence. These are summarized in Table B.2.

Table B.2 Relevant Time Frames for the Loss of MFW Scenario

Time Frame	Major Occurrences	Potential Operator Influence
Initiator	Loss of MFW Reactor scram or turbine trip T_{avg} drops upon reactor trip Pressurizer level drops with T_{avg}	The trip may be the first warning. If so, the operators have no chance to affect the initiator. If the problem develops slowly, operators may identify MFW problems and manually trip the plant.
0-2 minutes	AFWS starts automatically, when steam generator (SG) levels shrink to low-low level SG pressure is controlled per self-actuating blowdown Other auto equipment responses	Operators verify initial plant responses (particularly those that are automatic such as lowering power level, etc.) per EOPs; particularly AFWS starts in this case. Operators may even manually start AFWS before it auto starts.
2 min-1 hour	Heat sink restored (SG levels) Plant conditions restabilize Some throttling or shutting down of equipment (e.g., AFWS) begins	Operators are expected to throttle and then shutdown some AFW pumps to avoid overfilling the SGs; or respond to lack of cooling (and enter other EOPs) if heat sink apparently not restoring. They perform other actions as necessary (e.g., pressurizer heater on or off) to keep plant stabilized.
>1 hour	Unnecessary equipment shutdown Achieve stable hot or cold shutdown	Operator shuts down unnecessary equipment and transitions plant to hot/cold shutdown if desired

The above summary indicates that in the first few minutes expected operator actions involve verification of expected, and typically automatic plant responses. In order for the operators to not respond, for instance, to an initial degradation or failure of AFWS (an example of HFE 2), a significant diversion believed to be extremely important is likely to be required in order for the operators to not notice or otherwise not respond to a failure to restore secondary cooling. Much later in the scenario, throttling back and/or shut down of equipment associated with secondary cooling is "expected." Therefore, deviations of interest that might cause HFE 1 would most likely need to involve the appearance that the requirements for these expected actions have been met when in actuality, they have not. Hence, these types of vulnerabilities should be considered for examination later in Step 6.

B.5.3 Operator Tendencies and Informal Rules

Of the operator action tendencies summarized in Table 9.12a, the tendency of most interest to the issue as defined in Step 1 is that involving the operators' tendency to decrease plant cooldown. Such a tendency could lead to the cut back or shut down of secondary cooling which is the issue of concern as defined in Step 1. Based on a review of Table 9.12a and of the formal steps in the EOPs,

observable plant indications that would strengthen the tendency to want to decrease cooldown and hence represent a vulnerability of interest include:

- pressurizer pressure is continuing to decrease or is lower than expected
- too much core heat removal (i.e., higher or faster than expected) as evidenced, for instance, by falling RCS temperatures
- steam generator conditions suggest too much cooldown, as evidenced by higher or faster rising generator levels than expected, and/or by declining or too low steam generator pressures

In addition to the above plant indications that tend to induce the action of decreasing cooldown, operators are also cautioned and trained to avoid excessive cooldown and the potential for entering the pressurized thermal shock regime. This training, based in both formal and informal rules, further supports the conclusion that any appearances of too rapid a cooldown could be a vulnerability that might induce HFE 1 especially.

In addition, there are two informal rules that may be particularly relevant to the HFEs of interest. These are:

- Protect equipment. Operators are acutely sensitive to signs of equipment degradation (e.g., fluctuating pump current reading) and rapidly shutting down this equipment if it is not deemed to be necessary. This sensitivity came about due to a recent incident in which a degrading main feedwater pump was not shut down in time to prevent serious damage and resulted in a costly repair. Deviations of the base case scenario involving apparent equipment degradation may induce the HFEs of interest.
- Lack of detailed knowledge of the subtleties of the instrumentation and control (I&C) circuits and their potential vulnerabilities and effects. Deviations of the base case scenario involving subtle I&C failures associated with the key indications or equipment responses may contribute to the likelihood of the HFEs of interest.

B.5.4 Evaluation of Formal Rules and Emergency Operating Procedures

This evaluation looks for vulnerabilities associated with ways the EOPs and other formal rules may lead operators to the HFEs of concern. The EOPs are the primary input to the operators' formal rules

for responding to a loss of main feedwater event. This examination is developed by tracking those portions of the plant's EOPs that are most germane to that type of scenario.

Figure B.13 (on two pages) displays in a simplified flowchart the portions of the EOPs most likely to be followed in the base case loss of main feedwater scenario as well as possible pathways to other EOPs if complications develop. Note that this simplified flowchart is not meant to duplicate the EOPs. However, it does show where (a) branch points from the most applicable procedure to other procedures, (b) where specific steps exist that call for stopping equipment that is particularly germane to the scenario, or (c) where a major reconfiguration of equipment is called out. Such places in the EOPs represent possible vulnerabilities where it may be more likely for the HFEs of interest to occur as a result of entering a wrong procedure, or where equipment might be shut down or reconfigured inappropriately. Where deemed beneficial, information is provided in Figure B.13 that summarizes the following:

- actions to be taken
- potential for ambiguity
- a judgment on the significance of taking the wrong branch or inappropriate action.

In addition to the information in Figure B.13, the EOPs also provide for continuous monitoring of "critical safety functions". EOP F-0.3 heat sink is most relevant to this scenario and requires monitoring of the following:

- feed flow rate (>200gpm?)
- SG levels (>4% in one or both SGs?; <67% in both SGs?)
- SG pressures (<1130 psig or <1070 psig in both SGs?)

Depending on the outcomes of these decisions, other function recovery procedures may need to be entered if additional complications occur during the scenario. These other procedures generally call for increasing or decreasing the heat sink capability. Note that too much cooldown while at high RCS pressure could cause entrance into the pressurized thermal shock regime, which the operators are trained to avoid. Too little cooldown could cause heat buildup in the RCS, along with further recovery complications or even core damage.

A review of the above portions of the EOPs for potential vulnerabilities that might lead to the HFEs of interest suggests the following observations:

- Any deviation scenario that contains the following characteristics is of interest:
    - too much cooldown during the scenario, which if false or otherwise interpreted inappropriately, could cause the operators to over-react and cut back feed flow or secondary cooling
    - too little cooldown during the scenario, which if not addressed in a timely manner due to resource diversions caused by other complexities, could cause further heatup in the RCS or even core damage.

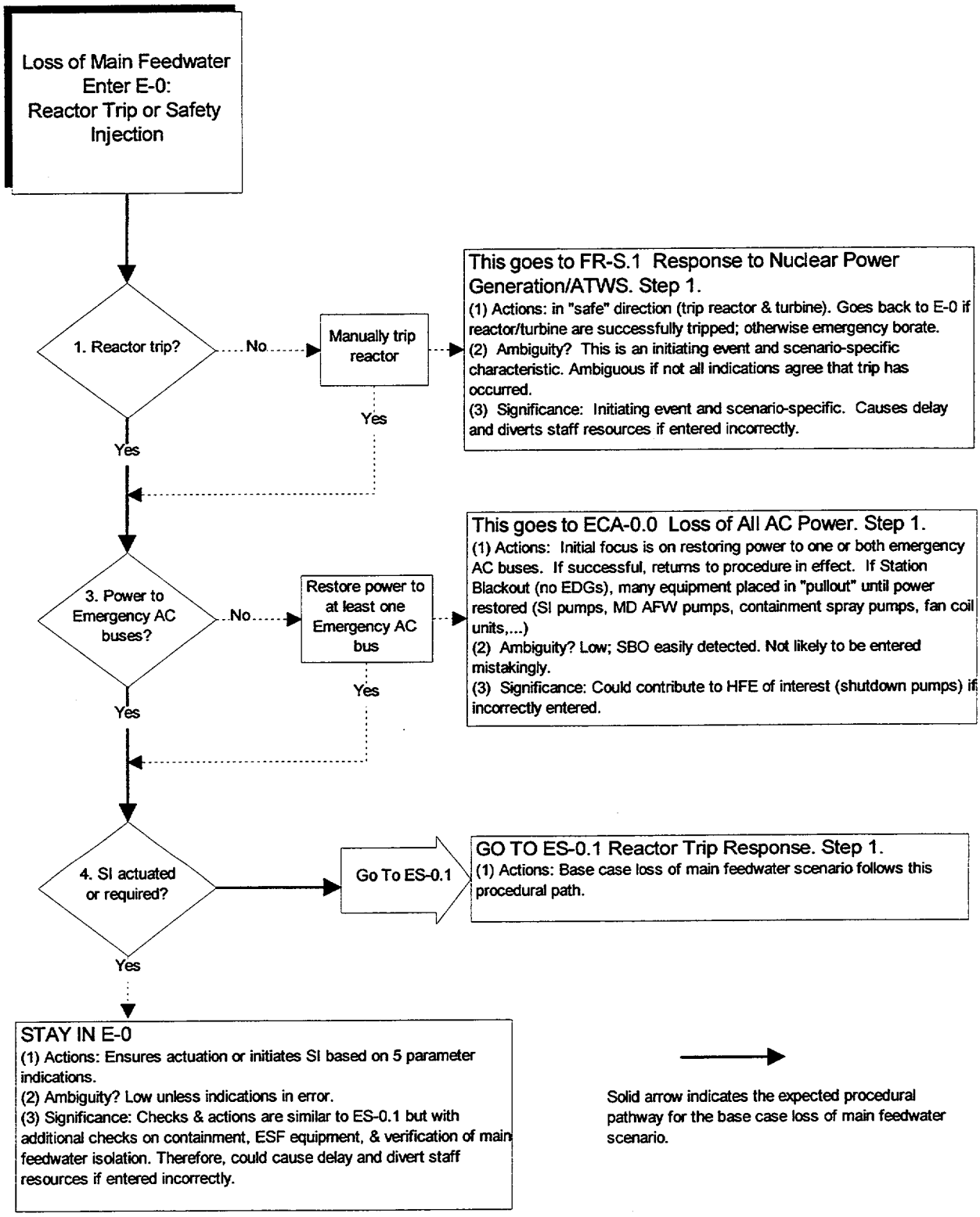


Figure B.13 EOP Highlights Related to Loss of Main Feed Scenario

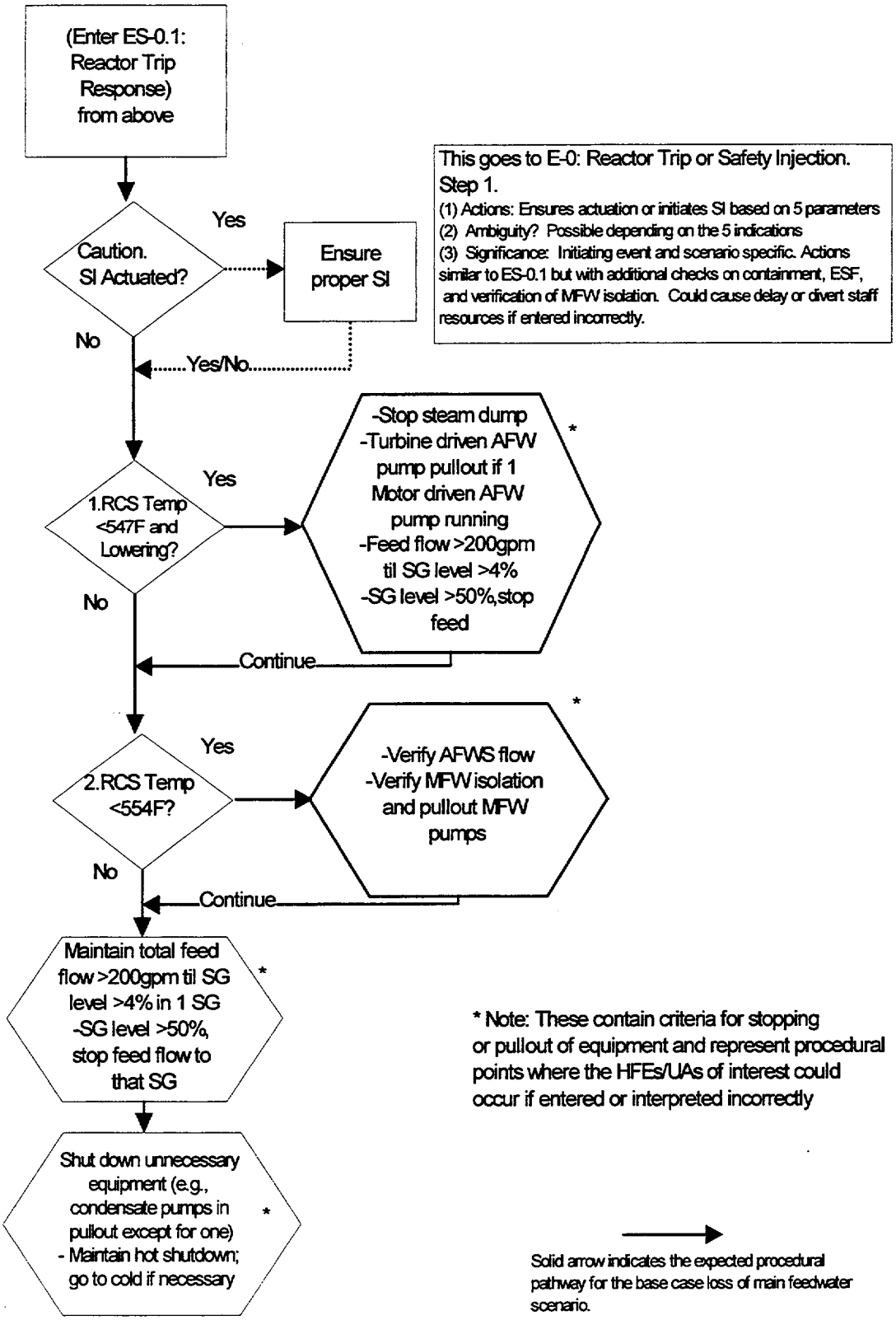


Figure B.13 EOP Highlights Related to Loss of Main Feed Scenario (continued)

- It does not appear that failure of reactor trip (actual or falsely indicated) would necessarily induce the HFEs of concern other than because it could compete for operator attention and hence resources. Most actions invoked by FR-S.1 would likely require operators to ensure even more secondary cooling, not less, because of the higher power levels involved if failure to scram were to occur. Other HFEs could certainly result because of operators attempting to deal with a much more complicated situation, but they are not the subject of this analysis. Only because of the possible competition for operator resources, will this form of complication to the base case scenario be further considered.

- If an actual or perceived blackout were to occur, actions involving "pullout" of equipment are called for, including motor-driven auxiliary feedwater pumps. Because of the possibility of inappropriately diagnosing a blackout or of failing to restore secondary cooling equipment following blackout recovery, further investigation of partial or total losses of electric power as a complicating factor in the scenario that might induce the HFEs of interest seems appropriate. This and other complicating failures of support systems may warrant further consideration.

- Safety injection, especially if falsely required, will likely add to cooldown of the plant and if deemed unnecessary, might induce actions to reduce the cooldown and possibly the HFEs of interest (especially HFE 1). Further investigation of this complication in the base case scenario seems warranted.

- Sufficiently low temperatures in the RCS and/or subsequent shutdown actions call for steam generator feed flow to be reduced and eventually stopped if sufficient generator levels are reached. False indications or similar complications might induce the HFEs of interest (especially HFE 1), and are worth further investigation.

This information is revisited during the deviation analysis in Step 6 to assist in determining the likelihood and significance of taking wrong branches or inappropriate actions because of the deviation.

B.5.5 Summary of Potential Vulnerabilities

The traits of possible deviations from the base case scenario (to be developed in the next step) that take advantage of the potential vulnerabilities and possible pitfalls identified in this step include the following:

- complexities involving other (nontrained or infrequently trained) equipment failures, subtle dependent failures, or other reasons for unexpected abnormalities

- indications of too much cooldown, as evidenced, for instance, by low pressurizer pressure, low RCS temperatures, high steam generator level, low generator pressures

- indications of equipment degradation that may provoke equipment shutdown

- complexities that seriously compete for operator attention and hence resources
- the possibility of a perceived blackout, other electric power anomalies, or other support system faults, particularly if they have subtle effects
- the possibility of a safety injection, especially if falsely indicated as required, that might induce actions to reduce the cooldown.

B.6 Step 6: Search for Deviations from the Base Case Scenario

In this step, ways in which the plant and operator response might deviate from the base case scenario are identified. Of interest are those deviations that may contribute to "error-forcing" situations such that the HFEs of concern become quite plausible.

The following is a series of searches for possible deviations and related contexts from the base case scenario that could induce the HFEs/UAs of interest as a result of the potential vulnerabilities identified in the previous step (Step 5).

B.6.1 Search for Initiator and Scenario Progression Deviations from the Base Case Scenario

The search for possible scenario deviations that make the HFEs/UAs more likely is begun by first considering deviations in the initiating event itself as well as in the scenario as a whole. In this case, a useful approach is to apply guide words typical of HAZOPs to investigate differences relative to the base case event involving loss of main feedwater. The base case loss of main feedwater is assumed to be an abrupt and total loss as the initiating event, followed by successful operation of all mitigating systems (safety and nonsafety). The following discussion documents possible types of deviations associated with the initiating event and the scenario progression.

Table B.3 shows the possible deviations that have been considered in this search. The types of initiator or scenario deviations that seem to have the most potential for inducing the HFEs/UAs of interest involve confusion as to the true status of the main feedwater system and whether it is sufficient to remove decay heat, as well as equipment malfunctions during the plant response.

Table B.4 summarizes more specifically how deviations carried forward from Table B.3 might "trigger" relevant cognitive processes, error mechanisms, and related error types based on a review of Tables 9.15a and b as well as 9.16a and b, in ways that might induce the HFEs/UAs of concern. For the possible physical deviations being considered, the contents of Tables 9.15a and b and 9.16a and b most relevant to the HFEs/UAs of interest are shown in the second column of Table B.4. The third column of Table B.4 summarizes the potential errors that could occur, considering the general error types provided in those tables. For the slower/partial/repeated type of initiator deviation, slower than expected parameter changes enhanced by the "belief" that the situation has become stabilized with main feed flow (potentially incorrect situation assessment) could make either HFE 1 or 2 more plausible (i.e., success is anticipated and so action to "disable" AFWS could be taken too soon). For instance, if a degradation of MFW is sufficient to cause a reactor trip on steam/feed

Table B.3 Loss of MFW Initiating Event: Scenario Deviation Considerations

Guide Word	Possible Physical Deviation	Significance	Carry Forward in the Analysis?
No/not/never	Initiator - N/A Scenario - multiple equipment failures	Relative to the initiator, "no" loss of main feed eliminates the initiator and so there is no event. Use of this guide word is not applicable. Relative to the scenario, these guide words are used to address "no" overall plant response (never) to the event (e.g., no RPS and no AFWS and...). Such a case is considered too improbable.	No.
More/early/ quicker/ shorter	Initiator - N/A Scenario - starting steam generator levels, response of automatic or nonsafety equipment differs from "expectations"	These constitute a quicker loss of main feed or subsequent plant response than assumed in the base case scenario. The base case scenario already assumes an abrupt and clearly discernible loss of main feed. Therefore, these guide words are not applicable to the initiator. The plant response might be somewhat quicker than operator "expectations" (such as that due to particularly high or low initial steam generator levels and/or equipment malfunctions). Possible specific considerations will be addressed in the second search regarding parameter responses and relevant rules.	Consider equipment malfunctions and related parameter indications during the scenario in the second search regarding relevant rules.
Less/slower/ longer/late/ partial/ repeated/as well as	Initiator - MFW is not totally and abruptly lost initially, but is only partially, slowly, or repeatedly lost over time or involves an additional complexity. Scenario - starting steam generator levels, response of automatic or nonsafety equipment differs from "expectations"	For the initiator, this is a possible situation that could add confusion as to the extent or nature of main feedwater loss or raise doubt as to whether it is lost. Such confusion might enhance the chance of disabling or otherwise cutting back auxiliary secondary cooling before the nature and extent of the main feed loss are completely understood so that appropriate actions are taken. The plant response could occur more slowly, involve additional equipment failures, or cause partial or even repeated responses so as to be different than operator "expectations" (such as that due to particularly high or low initial steam generator levels and/or equipment malfunctions). Possible specific considerations will be addressed in the second search regarding parameter responses and relevant rules.	Consider a less than abrupt and total loss of main feed initiator Consider equipment malfunctions and related parameter indications during the scenario in the second search regarding relevant rules.

Table B.3 Loss of MFW Initiating Event: Scenario Deviation Considerations (Cont.)

Guide Word	Possible Physical Deviation	Significance	Carry Forward in the Analysis?
Reversed	Initiator - Main feedwater is apparently restored but it is still not sufficient or is later lost again (repeated). Scenario - equipment malfunctions occur later that reverse the earlier plant response trends.	For the initiator, this is a possible situation that could add confusion as to the extent or nature of main feedwater recovery. Such confusion might enhance the chance of disabling or otherwise cutting back auxiliary secondary cooling before the nature and extent of the main feed recovery are completely understood so that appropriate actions are taken. The plant response could involve later equipment failures so that recovery trends reverse and the plant degrades again. Possible specific considerations will be addressed in the second search regarding parameter responses and relevant rules.	Consider a less than total recovery of main feed. Consider late equipment malfunctions and related parameter indications during the scenario in the second search regarding relevant rules.

Table B.4 Results of the Loss of Main Feed Initiating Event: Scenario Deviation Analysis

Possible Physical Deviation	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
Main feedwater is not totally and abruptly lost initially, but is only partially lost or is lost slowly or repeatedly over time.	No change in parameters or a smaller change than expected. [No indication or slower or smaller than expected changes in plant parameters (e.g., steam gen. levels dropping less than anticipated since partial main feed available)] Starts as apparent simple, "garden path" problem, thereby triggering familiarity or even complacency. (Starts as partial loss of main feed but which could degrade and become more severe at some later time) Familiarity and simple expectations about the event need to be overcome if situation changes. (Situation could worsen over time, perhaps unexpectedly, requiring situation assessment and response change) Expectation bias (trained loss of MFW event) must be overcome because of dilemma. (With both MFW and AFWS potentially available, which to use as well as too little vs. too much cooldown represent possible tradeoffs or dilemmas as to the appropriate actions)	May take no action or delayed action to prevent further degradation of main feedwater. Not relevant to HFEs of interest. Could believe situation has stabilized (become static) with some MFW flow and thus assumed to not be very serious; so could disable or otherwise stop AFW too soon to avoid overfilling SGs or overcooling (as an overeager response to the dilemma/tradeoff between MFW and AFWS operation). Problem could later worsen if MFW subsequently and totally lost, requiring further detection and reestablishment of AFW, which could be missed if seriousness of new situation is not realized. Possibility of either HFE 1 or 2.	Yes. Should carry forward as a possible complication for the initiator due to the error mechanisms potentially "triggered" by such a physical deviation. Hence, this type of deviation should be considered in any deviation scenario of interest.
Main feedwater subsequently is partially recovered but is still not sufficient or is later lost again.	Familiarity and simple expectations about the event need to be overcome if situation changes or reverses. (Reversing parameter trends, requiring reassessment)	It may be difficult for operators to change their actions in response to changing MFW conditions. In particular, they could act too soon (overeagerness) to disable or stop AFW to avoid overfilling SGs or overcooling in the belief that MFW is sufficiently recovered. An example of HFE 1	Yes. Another example of a possible initiator complexity adding to an error-forcing context of potential interest in a deviation scenario.

Table B.4 Results of the Loss of Main Feed Initiating Event: Scenario Deviation Analysis (Cont.)

Possible Physical Deviation	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
Various equipment malfunctions that change the pace or sequence of events for the scenario	No change on a smaller change in parameters than expected. [No indication if slower/smaller than expected changes in plant parameters (e.g., steam gen. levels dropping less than anticipated)] Starts as apparent simple, "garden path" problem, thereby triggering familiarity or even complacency. (Starts as partial loss of main feed but which degrade and become more severe at some later time) Familiarity and simple expectations about the event need to be overcome if situation changes. (Situation could worsen over time, perhaps unexpectedly, requiring situation assessment and response change) Expectation bias (trained loss of MFW event) must be overcome because of tradeoff or dilemma. (With both MFW and AFWS potentially available, which to use as well as too little vs. too much cooldown represent possible tradeoffs or dilemmas as to the appropriate actions)	Operators may take inappropriate action or correct action too soon (overeagerness) in response to changing scenario. Of particular interest is delayed action on none in response to degrading secondary cooling condition (HFE 2) or action of cutting back cooling too soon (HFE 1). Specific scenario and related parameter differences and potential operator actions will be examined in second search.	Yes. Specific possibilities will be addressed in subsequent search.

flow mismatch but some main feed flow still exists so that steam generator levels are not yet sufficiently low to cause AFWS initiation (low-low level), operators might be induced to think that sufficient feed flow is available to handle post-trip cooling and therefore be inclined to prevent or quickly cut back AFWS flow. If this action is performed in a way that would prevent subsequent auto-start of AFWS such as by pulling to lock the pumps, any further degradation or subsequent total loss of main feedwater (a later change requiring a change in the situation assessment) may not be addressed by manually restarting AFWS in a timely manner, especially if there are other unrelated distractions while responding to the event. For the second type of initiator deviation involving a partial restoration (reversal) of main feedwater flow, a similar effect may be possible in that it might be assumed that the main feed is restoring secondary cooling, potentially causing premature shut down of AFWS. As for deviations related to scenario changes caused by equipment malfunctions, this universal type of deviation will be examined more closely in subsequent searches, especially the second search. In that search, plant parameter changes and hence relevant rule responses will be reviewed to identify specific and particularly troublesome scenario deviations.

Hence, because of the potential to be contributing factors to contexts that could make HFE 1 or 2 more likely, (a) a partial or slowly degrading (but not total) loss of MFW, (b) an event involving a partial but still insufficient recovery of MFW, and (c) an event involving malfunction complexities are all carried forward as a potential part of any deviation from the base case scenario that might induce either HFE 1 or 2.

B.6.2 Search of Relevant Rules

This portion of the analysis examines whether the HFEs/UAs of interest could be induced as a result of deviations from the base case scenario so that incorrect "rules" (provided primarily by the EOPs and other informal rules) are followed, or the EOP decision and action statements can be applied in ways that would cause the HFEs.

Figure B.13 and the related text presented: (a) the expected EOPs that would be entered in the base case scenario, (b) key decision points in those EOPs, and (c) a discussion of the most relevant critical safety function EOP, F-0.3, related to heat sink conditions. In stepping through the various EOPs shown in Figure B.13, EOP F-0.3, and subsequent EOPs that might be entered if further complications developed in the scenario, nothing was found that would directly cause the HFEs/UAs of interest simply by following the EOPs. Still, the following discussion summarizes the conditions in all these EOPs that would result in shutting down (at least temporarily or partially) secondary cooling:

- Generally, secondary cooling via flow to the SGs is to be maintained until the narrow range level in the SGs is at least 4%, at which point throttling back can occur, attempting to control level in the 4%-50% range.

- If SG narrow range level gets too high (>67%), isolate AFW flow to the affected SG.

- If SG pressure gets too high (>1130 psig) and cannot be decreased, isolate AFW flow to the affected SG.

- If an SG is determined to be faulted, as indicated by SG pressure decreasing in an uncontrolled manner or an SG is completely depressurized, it is isolated (note that at least one SG is suppose to be maintained for cooldown).

- If a station blackout is determined to be in progress, the motor-driven AFWS pumps are placed in "pullout" until power is restored.

- Whenever steam dumping is not warranted and the motor-driven AFWS pumps are running, the turbine-driven AFWS pump is shut down and placed in pullout, especially when the RCS temperature is less than 547°F.

- Main feedwater is also isolated under the above and other related conditions.

Besides the above "formal rules," one of the informal rule vulnerabilities mentioned in Step 5 is:

- Protect equipment. Operators are acutely sensitive to signs of equipment degradation (e.g., fluctuating pump current reading) and rapidly shutting down this equipment if it is not deemed to be necessary. Hence apparent equipment problems could further enhance the desire to not use or otherwise shut down secondary cooling equipment.

Based on the above summary, in order for either of the HFEs of concern to occur when following the EOPs or the above informal rule, one or a combination of the following must occur:

- SG levels are indicating higher than they really are or the operators perceive them as doing so.

- SG pressures are indicating higher than they really are or the operators perceive them as so.

- SG pressures are indicating lower or decreasing faster than they really are or the operators perceive them as doing so.

- Operators believe a station blackout is in progress and the turbine-driven AFW pump is also inadvertently shut down.

- The turbine-driven AFW pump is inadvertently shut down even when the motor pumps are not running.

- Trouble with secondary cooling equipment occurs, or is perceived as such, and operators shut down equipment that is actually needed.

Each of these conditions is examined in Table B.5. The potential error mechanisms affecting human response and subsequent error types come from review of the error mechanisms and related error types in Tables 9.15a and b and 9.16a and b (just as was done for the entries in Table B.4).

Table B.5 Results of Relevant Rule Deviation Analysis

Condition	Example Causes of the Condition	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
SG levels are indicating higher than they really are or the operators perceive them as doing so	Uncontrolled blowdown (e.g., MSSVs stuck-open) temporarily indicates high level	Familiarity and simple expectations about the event need to be overcome if situation changes. There is a change from the "expected" yet it can be explained by expectation that levels should rise. Overeagerness to respond in an inappropriate way may be possible.	If operator does not detect actual failure and wait for re-stabilized (sustained) condition, could inappropriately cut back feed flow based on eagerness to respond to temporary high levels	Yes.
	Multiple SG level indicators in error	Missing or misleading information could lead to wrong entry into procedure steps and "trigger" an eagerness to respond to seemingly high SG level conditions.	Could inappropriately cut back feed flow (overeagerness) based on erroneous but anticipated level indications.	Yes, but only if operator focuses on a few indications or a common-cause failure occurs. Otherwise, too many failures have to occur.
SG pressures are indicating higher than they really are or the operators perceive them as doing so	Multiple SG pressure indicators in error	Missing or misleading information could lead to wrong entry into procedure steps and "trigger" an eagerness to respond to seemingly high SG pressure conditions.	Could inappropriately cut back feed flow (overeagerness) based on erroneous pressure indications.	Yes, but only if operator focuses on a few indications or a common-cause failure occurs. Otherwise, too many failures have to occur.

Table B.5 Results of Relevant Rule Deviation Analysis (Cont.)

Condition	Example Causes of the Condition	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
SG pressures are indicating lower or decreasing faster than they really are or the operators perceive them as so	Temporary blowdown system malfunction or uncontrolled blowdown (MSSV stuck open then recloses)	Familiarity and simple expectations about the event need to be overcome if situation changes. Unexpected but large or fast change in parameter may cause preoccupation with this parameter (tunnel vision) and eagerness to respond	If operator does not detect actual failure and wait for re-stabilized (sustained) condition, could inappropriately cut back feed flow based on eagerness to respond to temporary low or decreasing pressure	Yes.
	Multiple SG pressure indicators in error	Missing or misleading information could lead to wrong entry into procedure steps and "trigger" an eagerness to respond to seemingly low SG pressure conditions.	Could inappropriately cut back feed flow (overeagerness) based on erroneous pressure indications.	Yes, but only if operator focuses on few indications or a common-cause failure occurs. Otherwise, too many failures have to occur.
Operators believe a station blackout (SBO) is in progress and the turbine-driven AFW pump is also inad-vertently shut down	Numerous false indications of SBO	Missing or misleading information could lead to wrong entry into procedure steps and "trigger" an eagerness to respond to seemingly SBO conditions	Seems it would also require a slip to shut down turbine AFW.	No. Seems unlikely to misdiagnose SBO and make slip as well.
The turbine-driven AFW pump is in-advertently shut down even when the motor pumps are not running	Erroneous indications of motor pump operation	Missing or misleading information could lead to wrong entry into procedure steps and "trigger" a response to shutdown turbine.	Seems it would also require a slip to shut down turbine AFW	No. Seems it would require multiple indication failures and maybe even require distractions–improbable.

Table B.5 Results of Relevant Rule Deviation Analysis (Cont.)

Condition	Example Causes of the Condition	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
Equipment trouble induces shutdown by operator	Indication of equipment trouble	Training bias; informal rule, protect equipment. "Double bind"– maintain cooling vs. shutting off equipment	May take inappropriate action to shut down needed cooling equipment.	Yes

Based on the Table B.5 summary, it appears that the operators could inappropriately shut down or otherwise prevent proper secondary cooling and thus render HFE 1 or 2, primarily if (a) a temporary condition arises that indicates it is appropriate to throttle back or shut down secondary cooling flow and the operators do not wait for conditions to restabilize, (b) multiple indication failures for at least one parameter (e.g., level) exist, (c) a significant distraction due to other complications occurs and operators anticipate or otherwise misread parameter indications, (d) evidence of equipment trouble occurs, which if false or not critical could possibly induce inappropriate shutdown of the equipment, or (e) a combination of these. Note that in the case of erroneous indications, additional factors related to operators tending to focus on a single parameter (due to training or other crew tendencies) will likely be part of the context. These possible deviations are carried forward in the analysis to be considered in any context that might induce either HFE 1 or 2.

B.6.3 Search for Support System Dependencies

A review of the support system dependencies from the PRA for the plant revealed that a number of support system faults during the event could add to the complexity of the scenario and thus potentially contribute to any error-forcing context. Of all the support system faults that might occur coincident with a loss of main feedwater event (involving equipment cooling; heating, ventilation, and cooling; instrument air; electric power), loss of power is of most interest since it has the potential to contribute to the cause of the initiator, fail some of the responding equipment, potentially cause erroneous indications, and add to the complexity associated with the scenario, all at the same time.

In considering the ways an electrical power disruption might occur, two broad categories are addressed. The first is a plant-wide disruption, exemplified by a loss of offsite power. The second is a loss of only one or two buses, thereby affecting only portions of the plant systems and/or indications. Each of these conditions is examined in Table B.6. The potential error mechanisms affecting human response and possible error types come from review of Tables 9.15a and b and 9.16a and b.

A plant-wide electric power loss is likely to be easily detected (for instance, control room lights go out) and is one that operators are trained on from time to time. Such a deviation is probably more "unexpected" if it is delayed and happens later during the response to an event. When a widespread loss of power happens, interruption of operating equipment also occurs. Depending on diesel starts or subsequent power recovery, the crew looks for restarting of important mitigating equipment or attempts to manually start equipment. If the loss of power is delayed and occurs some time after the occurrence of the initiating event, it may be even more "unexpected" than if it occurred as part of the initiating event. Furthermore, if emergency diesel power also all fails, then only the turbine-driven AFWS pump train can operate until at least limited power is restored. Per the EAC-0.0 procedure in the case of station blackout, much mitigating equipment is placed in "pullout," which could delay or even prevent a mitigating equipment response once power is restored, depending on the crew's response (or lack thereof, which could be unsafe acts) to reactivate the equipment. Even if diesel power is established, operators could miss or at least be delayed in ensuring that sufficient equipment has reactivated and proper recovery of plant conditions is occurring. In addition, further complications occur such as loss of pressurizer heater and spray control. A particularly important unsafe act could be the failure to ensure proper restoration of AFWS equipment following the power loss.

Table B.6 Results of the System Dependency Deviation Analysis

Condition	Example Causes of the Condition	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
Widespread loss of electrical power	Loss of offsite power to the plant	Complacency and expectations about the event need to be overcome if situation changes. Focused attention or obsession on power loss and diesel start or power recovery (tunnel vision) may be possible. If loss occurs later in scenario, must respond to late change in situation.	May draw attention away from ensuring proper actions concerning restoration of AFWS	No. Next condition seems more problematic.
Partial loss of electrical power (e.g., instrument buses that serve SG level indications)	Instrument bus fault	Complacency could lead to missing the fault if indications of fault can be subtle or non-compelling. Fixation or focused attention or obsession on power loss (if detected) and power recovery may occur. Plant-unique feature of some SG levels failing to midscale will further the likelihood to cut back AFWS.	Lack of awareness of subtle failure or unrecognized effect on indications could lead to incorrect assessment of secondary cooling status or failure to recognize serious situation. May also draw attention away from ensuring proper restoration of AFWS	Yes, because as the fault indication is subtle and "triggers" a unique plant failure of some SG level indicators to midscale (could be particularly troublesome).

The second class of deviation addressed in Table B.6 could be more subtle, harder to detect, and therefore represent an even greater challenging context. This is the loss or degradation of one or two electrical buses, either as part of the initiator or as a delayed event some time after the initial response of the plant. Detection could be harder or at least delayed because the loss is not widespread and may be at a level within the electrical network that is not specifically alarmed or indicated (i.e., covered only by a general alarm). While such a "partial loss" of electrical power in the plant would seemingly not cause the crew to follow EAC-0.0, the operator tendencies are similar (attempt to recover the power if detected) and the plant response is more complicated because of the need to detect and respond to the effects of such partial losses of electrical power.

Depending on the specific buses lost, some indications could also be affected, further complicating the ability of the crew to understand the status of the plant. For instance, at this plant, failure of a particular set of instrument buses has been found to lead some steam generator level indicators to fail to midscale, a situation that could be particularly troublesome in ensuring proper heat sink conditions. This plant-unique finding along with the operators' tendency to focus on the steam generator level as a key indication of the status of secondary cooling (discussed in the previous step), together could provide an interesting element of an error-forcing context should any of the instrument buses fail.

In both cases, the tendency to attempt to recover power is not necessarily unsafe as long as it does not divert attention too much from the overall plant status and restoration is not attempted while an electrical fault still exists. Should the latter situation be the case, attempts to restore power could cause repeated failures to restore equipment or even expand the effect of the lost bus by tripping other buses when power recovery is attempted.

Table B.6 and the related discussion suggest that a loss or degradation of main feedwater coupled with a loss of power could provide a form of deviation from the base case scenario that could hamper the plant and crew response. If such a failure could either (a) actually cause a temporary rapid cooldown of the plant or (b) even worse, cause the appearance (falsely) of a rapid cooldown of the plant, there appears to exist the possibility of the crew cutting back too soon or even stopping AFWS flow if RCS temperatures appear to drop below that indicated in ES-0.1 and/or if SG levels appear to rise to too high a level (as caused by the midscale reading). There appear to be potential opportunities to throttle or even place much of the AFWS in "pullout," thinking that too much cooling is occurring (the potential unsafe act). If such steps were to be taken inappropriately, SG conditions could once again become degraded, requiring the operator to restore AFWS. Failure to do so in a timely manner (a potential unsafe act) could cause heatup of the RCS and even core damage if the condition persists.

Therefore it is suggested that a particularly challenging deviation associated with electrical power, and having the following characteristics, appears worth further review in subsequent steps in the ATHEANA process:

- a delayed failure of an instrument electrical bus in the plant

- the selected bus fault should disrupt cooldown control (if possible to further complicate the cooldown issue), and cause the affected SG level indicators to fail to midscale (in addition, one or two SG level indicators could also be removed from service, such as for calibration, as part of the total context)

- to further ensure the appearance of too rapid a cooldown, an actual but subtle and temporary cause for cooldown may also need to be part of the context, such as a leaking pressurizer spray valve

- the bus failure is such that a fault condition continues to exist, thereby hampering its restoration and becoming a further diversion of resources and attention

The above combined conditions could have the following characteristics:

(1) Indication of too rapid a cooldown (to further strengthen the tendency to decrease cooldown) as evidenced by decreasing (more than expected) pressurizer pressure, level, and RCS temperature indications. (This could be caused by a leaking pressurizer spray valve, for instance.)

(2) A rise in "some" of the steam generator level indicators (to midscale) caused by electrical bus failure. (This could falsely indicate that sufficient steam generator levels have been reached to allow cutback/shutdown of secondary cooling.)

(3) Together these indications may compel the operator to perform HFE 1.

A coincident bus failure could similarly be a contributing factor to HFE 2 to the extent that if it contributed to the appearance of a rapid cooldown while in fact there was a partial or total loss of secondary cooling due to equipment faults, actions might not be taken (or at least be significantly delayed) to restore the lost function. In such a case, the context would have the same characteristics as listed above but with the additional actual failure of secondary cooling as part of the scenario.

B.6.4 Search for Operator Tendencies and Error Types

This portion of the search process for possible deviations of the base case scenario is approached by keying on categories of deviations that may make the HFEs of concern more plausible based on certain human behavioral tendencies. From the information provided on general tendencies in Table 9.12a, it is evident that one of the operator tendencies is of particular interest to this analysis. It involves the scenario appearing to have the indications of overcooling so that the operator behavioral tendency for decreasing core cooling is intensified. Table B.7 summarizes information regarding this operator tendency, which has already been somewhat addressed in the previous searches.

Relative to HFE 1, the formal steps in the various EOPs that call for throttling back and eventually shutting down secondary cooling flow were addressed in a prior search. Hence any deviation that

Table B.7 Summary of Deviations Involving Operator Tendencies

Condition	Human Behavioral Tendency	Significance	Further Analysis?
Indication of overcooling (real or falsely indicated)	Slow down or stop overcooling	If inappropriately diagnosed, might induce action illustrative of HFE 1	Yes.

might cause HFE 1 must: (a) falsely indicate these required conditions have been met, (b) make an actual cooldown appear sufficiently threatening that in spite of the above requirements the operators incorrectly reduce or shut down secondary cooling, or (c) a combination of these characteristics.

Other supporting evidence might include evidence of falling pressurizer and steam generator pressures, significant subcooling readings, shrinking pressurizer level, etc. This is illustrated in Figures B.14a and b where multiple parameters indicate levels other than that normally expected in the base case loss of main feed scenario. The more evidence there is of a rapid cooldown, the more likely the operators will believe that this is the case and the stronger will be their tendency to stop the cooldown.

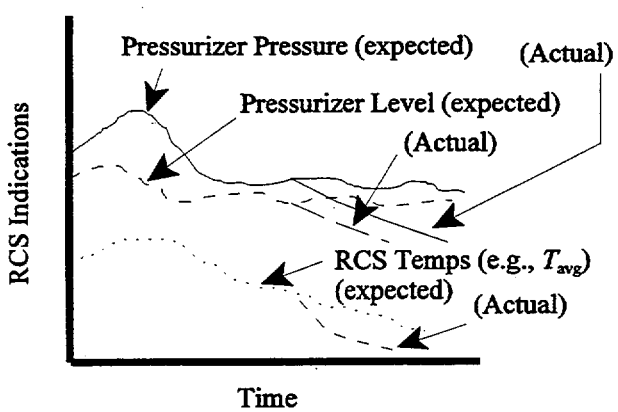


Figure B.14a RCS Response vs. Time

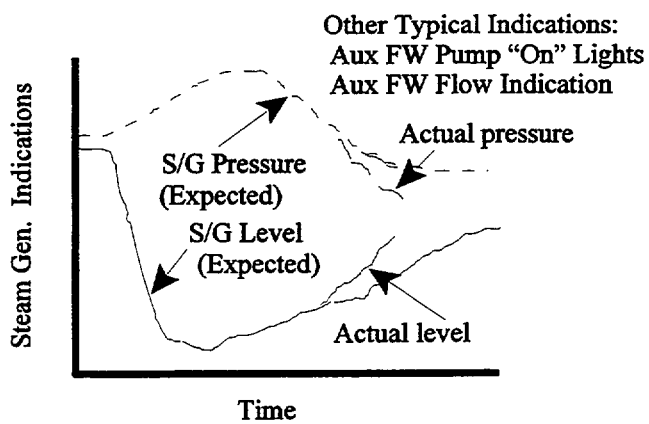


Figure B.14b SG Response vs. Time

As for an actual cooldown situation, such a deviation from the base case scenario must not be sufficient to ensure continued and adequate cooling of the core over the long term, or only be temporary. Further reenforcement of the need to cut back secondary cooling might exist if at least some of the steam generator indications falsely indicate that the requirements for throttling or shutting down feed flow have also been met. There are many ways that a cooldown may initially become greater than desired or anticipated, though not sustained. As for hardware faults associated

with the RCS, possible excessive cooldown might initially be caused by such failures as a demanded and stuck open PORV, a faulty operating pressurizer spray (e.g., stuck-open or leaking spray valve), an RCS leak or break, or a loss of pressurizer heater function, among others. Faults in the secondary plant with a similar effect might involve too rapid an initial steam generator blowdown such as that due to malfunction of the blowdown control system or a demanded and stuck-open main steam safety relief valve. Initial heat loss such as through a PORV, RCS leak, or malfunction in the secondary plant, or the addition of a cooling effect such as the pressurizer spray malfunction, could initially indicate that excessive cooldown is in progress.

In such cases, the operators' first priority is to search for the reason for the cooldown and if they find it, attempt to isolate or otherwise recover from the cause of the cooldown. It seems unlikely such a cooldown by itself would induce HFE 1 unless the source of the cooldown could not be identified. Hence, a subtle source of the cooldown would be more likely to contribute to an error-forcing context than an easily detected cause. If there was the added difficulty of at least some false steam generator indications, the context might be even more convincing.

In addition to the above, Tables 9.15a and b and 9.16a and b were reviewed for additional complicating factors (e.g., possible impasses, "red herrings") or error mechanisms (e.g., apathy) and related error types that might be "triggered" by possible scenario deviations that would induce human response tendencies similar to the HFEs of interest. No deviations other than those already addressed by this and the previous searches have been identified at this time.

In summary then, it would seem that the operator tendency to over-react to a seemingly rapid cooldown event and thus cause HFE 1 would need to involve:

- multiple indications of failures so that a rapid cooldown is falsely inferred, particularly if operators are also preoccupied with the one or two false parameters (especially steam generator level), or
- an actual but nonsufficient or temporary cooldown to which the operators respond inappropriately by not waiting long enough for conditions to stabilize, or
- a combination of the above conditions

B.6.5 Summary Description of Deviation Scenarios

The above searches have all contributed to the identification of the characteristics of a number of contexts that could make HFE 1 or 2 more plausible in a scenario involving an initial loss or degradation of main feedwater flow during normal plant operation. Based on these searches and the recognition that certain characteristics were repeatedly identified, it can be stated that the plausibility of the HFEs depends on deviation scenarios containing the following major elements to create a relevant error-forcing context:

- for HFE 1, there is a conflict over whether overcooling or undercooling is occurring so that overcooling appears to be the greater concern

- for HFE 2, a significant diversion occurs so that a delayed loss of secondary cooling is not addressed in a timely manner

- for both HFEs, malfunctions occur is key indications as to the degree of cooling (e.g., steam generator levels) so that both HFEs are more likely

In deviation scenarios with the above contexts, the likelihood of the HFEs would be much higher than normally expected. The most relevant error mechanisms and error types potentially "triggered" by such contexts are summarized in Table B.8, based on information developed in the prior searches. For instance, the conflict of over- vs. undercooling concerns brought about by the EOPs, other procedures, and related operator tendencies (supported by training) potentially "triggers" a fixation on this concern and the desire to avoid overcooling nearly as much as undercooling. Operator training, the EOPs, and the heat sink functional recovery procedure produce a significant reliance on indication of the steam generator level, thereby potentially setting up tunnel vision with regard to this specific parameter and when to throttle or cut back secondary cooling. The desire to avoid overfilling the steam generators, thereby contributing to an overcooling transient, also potentially "triggers" an eagerness to throttle back secondary cooling once this function appears satisfied.

In addition, a number of specific occurrences that could cause the plant conditions in Table B.8 were identified during the ATHEANA searches. For example, the plant conditions identified could occur through the following chain of events:

<u>Deviation Scenario 1; Example chain of events</u>

Pre-initiator: Plant operating nominally at full power. At least one (or more) steam generator level indicator among the Division A indicators is being tested and calibrated. (This lessens the redundancy of steam generator level indications relied on by the crew for secondary cooling status and thus contributes to the overall context.)

Initiator: A degrading main feedwater flow event such as that caused by controller malfunction, regulatory valve failure, or some other similar situation occurs that does not immediately or completely cause the loss of all main feed. It is, however, sufficient to cause dropping steam generator levels and a steam-flow mismatch such that an auto reactor trip will occur. (This could cause some early confusion as to the availability of main feed and create some doubt as to the need for AFWS because of overcooling concerns.)

Early failures: Because the initial rise in RCS temperature and pressure will occur as the heat sink (steam generators) degrades, the pressurizer spray valve is expected to operate. In the deviation scenario, the spray valve "leaks" even though it is indicating "closed." (This becomes a source of hard-to-detect cooldown, thereby adding to the overall context and concern about overcooling.)

Table B.8 Deviation Scenarios

HFE	Overall Plant Condition	Most Applicable Error Mechanisms of Concern	Applicable Error Types	Comments
1	A scenario in which there is uncertainty about whether under- or overcooling is occurring Key indicator (e.g., steam generator levels) as to the degree of cooling suffers a fault so that it adds to the uncertainty by indicating sufficient cooling.	Sets up a "tradeoff dilemma" as to what to do when both MFW and AFWS seem available, causing a fixation on a possible overcooling event. Tunnel vision or a focus on steam generator level indicators on the basis of training and procedure biases. With normal expectation to throttle AFWS in loss of MFW events, potential eagerness exists about shutting down AFWS, especially if it appears SG levels have been adequately satisfied.	All of the identified applicable error mechanisms can contribute to inappropriate actions, taking correct actions too soon, or failing to take (or delaying) needed actions.	The overall plant condition and the error mechanisms potentially "triggered" by the condition could all support the possibility that the operators will perform an unsafe act indicative of HFE 1 (degrade or shut off secondary cooling) because they are concerned about overcooling and some faulty steam generator level indicators (some indicating midscale) make it appear that the shutoff conditions for secondary cooling have been met.
2	A scenario involving an initial degradation of MFW followed by partial success of AFWS A significant diversion occurs as part of the scenario, along with the key indicator problem A "late" failure of the remainder of all feed occurs	Sets up a "tradeoff dilemma" as to what to do when both MFW and AFWS seem available, causing a fixation on a possible overcooling event. Tunnel vision or a focus on the significant diversion. Potential complacency once the scenario has progressed to the point that the operators believe core cooling concerns are satisfied.	All of the identified applicable error mechanisms can contribute to inappropriate actions, taking correct actions too soon, or failing (or delaying) needed actions.	With an added uncertainty as to whether AFWS is really needed initially, such a plant condition with a significant diversion could lead to a delay or failure to restore AFWS following a "late" failure of all feed after the operators believe core cooling concerns are satisfied (especially with the added complexity of a faulty SG level indicator).

Early success: All other plant response is as "expected," with no failures. This includes complete response of AFWS.

Delayed failures: All other "normal" actions occur, but before both steam generator narrow range indications reach 4%, a delayed and complete failure of main feed (if it is still partially functioning) occurs coincident with a fault on an electrical bus that serves the steam generator Division B indicators. (This provides a common-cause effect that will cause the affected indicators to fail to mid-scale, potentially causing the true status of steam generator levels to appear to have reached adequate levels to throttle back or shut down all feed.)

The above chain of events making up the deviation scenario for HFE 1 develops a context that is expected to increase the likelihood of an unsafe action representative of HFE 1 in which steam generator cooling is cut back too soon. The scenario raises the possibility of the crew becoming overly concerned with the apparent and potentially increasing cooldown rate (caused by the leaking spray valve, which they may or may not detect, and the possibility of continued or rapidly recovered main feed) so that secondary cooling is throttled back (via various means such as throttling or shutting down AFWS pumps or cutting back the steam dump) *before* the proper criteria have been met (unsafe acts illustrative of HFE 1). The likelihood is further increased by the inaccurate SG levels caused by both the unavailability of some indicators due to test and calibration as well as the instrument bus loss.

There are certainly other specific ways to create a deviation scenario that will have effects similar to the one described above. They all, however, should provide a context of confusion as to the status of main feed, provide an actual or apparent increase in the "expected" cooldown rate, and take advantage of the crew's tendency to rely on indicators of steam generator level. What is being postulated is a form of scenario that makes the plant status indicators respond much like that depicted in Figures B.14 a and b relative to "expectations." It is believed that this type of deviation scenario increases the likelihood of operators cutting back or even shutting down secondary cooling (via various means) *before* the proper conditions have been met and are stabilized.

<u>Deviation Scenario 2; Example chain of events</u>

Pre-initiator: Plant operating nominally at full power. At least one (or more) indicator of steam generator level among the Division A indicators is being tested and calibrated. (This lessens the redundancy in steam generator level indicators relied on by the crew for secondary cooling status.)

Initiator: A degrading main feedwater flow event such as that caused by controller malfunction, regulatory valve failure, or some other similar situation that does not immediately or completely cause loss of all main feed. It is, however, sufficient to cause a drop in steam generator levels and a steam-flow mismatch so that an auto reactor trip will occur. A few minutes following the trip, the main feed fails totally if it has not already been isolated. (This could cause some early confusion as to the availability of the main feed.)

Early failures: One of the two AFWS motor pumps fails on demand (nonrecoverable).

Early success: All other plant response is as "expected," with no failures.

Delayed failures: All other "normal" actions occur up to and including the expected shutdown and pull-to-lock of the turbine-driven AFWS pump, leaving one motor pump operating. Before the motor pump, is also shut off, a fire or failure occurs in an instrument bus (with a fire alarm) that will cause failure of some of the redundant Division B indicators of steam generator level. (This will be a potentially significant diversion as well as cause the affected indicators to go to midscale, thereby inaccurately indicating the status of the SG levels, just as in the scenario for HFE 1.) A few minutes later, with no warning, the running AFWS train fails, possibly with a noncompelling signal indicating failure of the injection path.

The above chain of events making up the deviation scenario for HFE 2 develops a context that is expected to increase the likelihood of an unsafe action representative of HFE 2 in which steam generator cooling is not restored or is restored too late following its "late" loss. The example scenario adds a potentially significant diversion regarding the fire that occurs as part of the instrument bus fault. The likelihood of not adequately responding to the late loss of all secondary cooling may be increased by the inaccurate SG levels caused by both the unavailability of some indicators due to test and calibration as well as the instrument bus loss and the diversion of attention to the fire.

There are certainly other specific ways to create a scenario that will have effects similar to the one described above. They all, however, should provide a context of a significant diversion (in this case the fire), a delayed failure of all secondary cooling once parameters seem to reach nearly recovered conditions, and take advantage of the crew's tendency to rely on indicators of steam generator level. It is believed that this type of deviation scenario increases the likelihood of operators not responding

to the total loss of secondary cooling since it happens unexpectedly "late" in the event and in the context of a competing diversion.

B.7 Step 7: Identify and Evaluate "Complicating Factors" and Links to Performance Shaping Factors (PSFs)

The deviation scenarios, as described above, already include a number of the types of additional complicating factors discussed for this step in Section 9. These include:

- degraded equipment operation, such as the initial degraded MFW condition
- instrumentation unavailabilities and anomalies (for steam generator levels) adding potential confusion about the plant's status

- the crew's tendency to rely on steam generator level as a single key indication of secondary cooling status as a result of existing training and procedure biases that focus on these levels as an indication of heat sink adequacy

- other hardware failures potentially causing diversions of the crew's attention and resources (particularly the bus fault in the first scenario and the bus fire in the second scenario), thereby adding to the workload and attention load of the crew. This could strain communication among crew members and add to the likelihood of the HFEs

One additional PSF that is being "triggered" in the described scenarios is the potential unawareness of the specific effects of the bus fault. Since it is expected that most crew members would not realize that the steam generator level indicators have been affected, this could lead the crew to believe that the levels are indeed adequate and it is time to shut down secondary cooling.

All of these complicating factors are considered to be already present by virtue of the deviation scenarios as they have been defined, and hence the factors support the likelihood that the HFEs might be committed in such circumstances.

B.8 Step 8: Evaluate the Potential for Recovery

Even if the scenarios and subsequent human failure events occur as postulated in the previous steps, there is a chance that the operators will recover from the degrading plant conditions before serious damage results. The possibilities for recovery include restoration of secondary cooling before dryout of the steam generators, or the restoration of feed in time to ensure sufficient core cooling. If neither is performed, core damage could occur, initiating in about 1 hour following the loss of secondary cooling.

For the postulated scenarios, and assuming the HFEs occur, the plant conditions will deteriorate since secondary cooling is not available to remove heat from the reactor coolant system. Various cues of this deteriorating condition should eventually become available. These are indicated by the simplified plots in Figure B.15 and the anticipated scenario progression log in Table B.9.

As summarized in the scenario progression log, the key to a rapid recovery of the degrading condition is the crew's assessment that the SG levels are in fact falling from an already "low" condition and that many of the SG level indicators are actually malfunctioning. Actions that could increase the likelihood of diagnosing the actual SG level conditions include placing the tested channel indicators back into service, identifying the effects of the faulted bus on the SG level indicators, or otherwise conservatively responding to any confusion about the true status of the SGs. If a diagnosis of the actual lowering of SG levels not made (which is still likely because of the original belief that SG levels are adequate, which contributed to the HFEs in the first place), other parameters indicating the condition of the RCS will appear "nearly normal" for a time until the RCS begins to heat up again. Once it does, the potential for operator recovery is spurred by the desire to

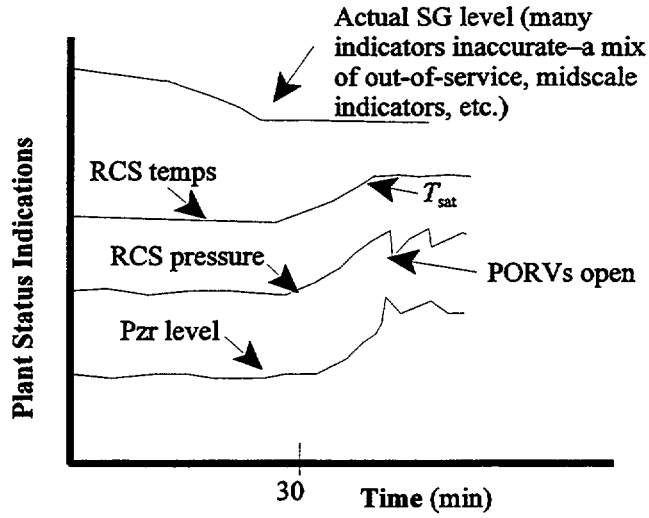


Figure B.15 Plant Status after HFE Occurs

find the reason(s) for the unexpected RCS conditions. During this time, the functional recovery procedures largely call for adjusting charging or letdown flow and similar actions. However, if the severely degraded SG level condition is still not diagnosed, RCS conditions will worsen. Once the SGs are dry, recovery is further hampered since any restoration of secondary feed is limited by an allowable flow rate at first, as a result of the dry SG conditions, and sufficient primary system cooling is difficult to obtain once the secondary heat sink is unavailable.

In summary, recovery from the original HFEs is possible if the actual degrading SG condition is diagnosed early in spite of out-of-service or otherwise malfunctioning indicators of SG level. However, the subtle failure of these indicators may make such a diagnosis difficult. Without such a diagnosis, RCS conditions are likely to get quite bad before sufficient evidence exists (in the form of an RCS void indicator and/or core thermocouple readings) for the crew to recover. By that time, recovery will be hampered by the "lateness" of the attempted recovery due to uncooperative thermal hydraulics.

B.9 Quantification Considerations

While much has been learned from the above analysis about the potential for the HFEs of interest to occur and the types of deviation scenarios that may increase the likelihood of the HFEs, it may be desirable to obtain a quantitative approximation as to the overall likelihood of such an occurrence.

In Section 10 it is seen that such an assessment requires estimating the frequency of the error-forcing context (made up of the frequency of the plant condition occurring × the probability of relevant PSFs), the probability the crew will perform the unsafe act(s) illustrative of the HFE, and the probability that the crew will not recover from their original mistake by the time serious damage to the plant occurs. Each of these is discussed and estimated below.

Table B.9 Scenario Progression Log Regarding Possible Recovery from HFEs

Approx. Timing after HFE Occurs	Symptom	Actions
0–30 minutes	Few (if any) steam generator level indicators show the actual lowering of SG levels as a result of no feed. Some indicators are being calibrated and tested and others show midscale readings from the failed bus.	Depending on the degree of confusion by operators' as to SG levels, they may (or may not) rush getting the SG indicators in test back into service and/or figure out the anomalies caused by the faulted instrument bus. If such actions are not taken, the crew may not immediately conclude that levels are dropping.
0–30 minutes	Other parameters are following "near normal" expectations (see Figure B.15) since it will take time for the steam generators to enough dry to cause re-heatup of the RCS. So for a while, there is little indication of the degrading situation.	Parameters remain within expected limits and thus no significant actions may be taken if the actual lowering of SG levels is missed.
30–60+ minutes	Parameters show the signs illustrated in Figure B.15 as the RCS heats up. RCS high-pressure, temperature, and pressurizer high-level alarms occur as RCS volume heats up and expands. PORVs eventually lift and quench tank alarms sound as well. If as the situation further degrades, reactor vessel level instrumentation system (RVLIS) void indication and core thermocouple readings will eventually indicate a very serious situation.	While actions will likely be taken to address the RCS condition problems, these will most likely involve checks or adjustments of charging or letdown flow. No significant core cooling restoration actions will be called upon by the functional recovery procedures until the RVLIS void fraction and eventual core exit thermocouples indicate a serious situation (if actual falling SG levels are not properly diagnosed). The RVLIS and thermocouple indications will likely occur well after the SGs are dry and primary cooling should have been established. Recovery at this late stage could be difficult.

B.9.1 Deviation Scenarios Challenging HFE 1

Frequency of Error-Forcing Context
The plant condition postulated to set up HFE 1 involves four elements that need to be quantified:

(1) frequency of a degraded MFW condition that causes the plant trip and eventually progresses to a total loss condition

(2) probability of an additional, small cooldown source, such as the suggested "leaking" spray valve

(3) probability that some SG level indicators are unavailable (e.g., as due to testing)

(4) probability that several SG level indicators fail but their failure is not readily apparent (e.g., the postulated drop to midscale caused by a bus loss

The frequency of the degrading MFW initiator condition is estimated using the current PRA information for the plant. The PRA documents the frequency of an initiating event with MFW available as approximately 2-year and the frequency of a transient involving a total loss of MFW as about 0.14 a year. Considering the in-between nature of the postulated deviation scenario involving a degrading and eventual total loss of MFW, it is assumed that such an event has a likelihood somewhere between the two PRA extremes and nearer the total loss frequency. Hence a value of 0.5 a year will be used to estimate the frequency of the postulated initiating event.

The probability of a small source of additional cooldown can be estimated from a couple of viewpoints. First, the probability of a leaking spray valve as postulated in the deviation scenario can be estimated from typical PRA data values for valves failing to close, which are around 3E-3 per demand. Considering the potential for a couple of demands of the spray valve, and recognizing that there are other potential sources of cooldown (e.g., letdown problems, pressurizer heater problems), an estimate in the E-2 range or greater seems reasonable. In addition, actual experience at this plant demonstrates overcooling concerns in about 1 out of 10 trips. Together, these viewpoints suggest a probability of 1E-1 as a reasonable estimate.

Most SG level instrumentation checks do not take long and only occasionally require recalibration during power operation. Plant experience indicates a probability that some of the SG channel readings will be unavailable at the time of the event as about 1E-3.

The probability of a loss of multiple SG level indicators so that their malfunction is not obvious (e.g., due to the postulated bus fault) can be estimated on the basis of typical inverter, bus, and similar equipment failure probabilities which from the plant PRA are as high as nearly 1E-4 per hour. Given that the failure must coincidentally occur probably during the first half-hour of the accident response, but that there are multiple equipment failures that could cause the same "bus loss" effect, a probability of 5E-4 is assigned.

The probability of many of the SG level indicators being simultaneously unavailable or faulted can be approximated by the above 1E-3×5E-4, or 5E-7. However, there may be other common cause failures not yet accounted for, such as lightning strikes, that may also cause multiple SG level indicators in both divisions to malfunction. To capture this additional possibility, a 1E-6 probability will be used to estimate the likelihood that multiple SG level indicators in both divisions are malfunctioning or otherwise misindicating.

Collectively, the above values multiplied together provide an approximation of the frequency of the postulated plant condition of about 5E-8 a year [0.5/year × 0.1 × 1E-6]. This is considered to not be a very likely scenario in light of other accident frequencies in the PRA, but not so small as to be insignificant either.

The probability that the relevant PSFs exist and are "triggered" by the plant conditions makes up the remainder of the overall frequency of the error-forcing context. As discussed in Step 7, it is believed that the training and procedure biases do provide a strong tendency towards "tunnel vision" on the SG level indicators for heat sink status. In addition, the crew would have to not recognize or otherwise not identify the potential bus fault effects at the time of the event. The PSFs are considered to be "triggered" as a result of the plant conditions and so the probability of the PSFs is assigned "1.0." Hence, the frequency of the error-forcing context is estimated at 5E-8 a year.

Probability of Unsafe Act(s) Illustrative of HFE 1

Given the plant conditions and PSFs above, it is the analysts' opinion that a very strong context exists for cutting back or shutting down secondary cooling in the belief that it has been adequately satisfied when it actually has not. As discussed earlier, the plant condition and PSFs will invoke the error mechanisms shown in Table B.8 that collectively all support the tendency to cut back cooldown. In spite of this strong context, however, performing the HFE is not judged to be "assured." Therefore, a 50-50 probability is assigned to this part of the quantification.

Probability of Nonrecovery

Section B.8 contains a discussion as to the recovery potential and notes that the greatest chance of success is judged to be associated with the recognition that the SG levels are indeed lower than originally believed by the crew. This could come about, for example, by restoring unavailable SG level indicators, restoring the bus (or other) fault causing the other SG level malfunctions, recalling the potential bus–indicator interactions, or other means. Since the other plant parameters will not provide early evidence of severe plant conditions, these are not likely to provide clues regarding the true heat sink condition.

Given the event, there could be some desire to reactivate SG level channels that are in test and to restore the failed bus or similar fault. Whether such actions would be done in time to recover from the original HFE depends on the ability to restore the equipment in a short time, and the extent of the personnel resources at the time, which could be a function of the time of day, etc. Even if the true SG level conditions are not diagnosed, the later symptoms of degrading plant status do prevent a late (but probably difficult) chance of recovery.

Considering all the above, it is difficult to derive a substantial basis for a nonrecovery probability since it depends on numerous factors, all of which are difficult to estimate as to their likelihood beforehand. Judgmentally, however, it seems hard to justify a nonrecovery probability lower than 10%-50% range, considering the strong tendency before and after the HFE to focus attention on SG levels (which may or may not be restored) and the lack of early cues from other plant parameters.

Frequency of the Entire Event Leading to Core Damage
Multiplying all of the above values together yields an overall frequency of such an event resulting in core damage, including the HFE and nonrecovery, in the E-9 per year range.

B.9.2 Deviation Scenarios Challenging HFE 2

Frequency of Error-Forcing Context
The plant condition postulated to set-up HFE 2 requires a combination of the initiating event, an eventual total loss of AFW (via a combination of failures and shutting down the turbine train), and the concurrent SG level anomalies that sufficiently challenge the operators so that they may not recognize and therefore recover the lost secondary cooling function. This involves five elements that need to be quantified:

(1) frequency of a degraded MFW condition that causes the plant trip and eventually progresses to a total loss condition

(2) probability that some SG level indicators are unavailable (e.g., due to testing)

(3) probability that one AFW train fails or is otherwise unavailable

(4) probability that several SG level indicators fail but that their failure is not readily apparent (e.g., the postulated failure to midscale caused by the bus loss) coincident with a strong distraction such as a fire (alarm)

(5) probability that the remaining motor AFW train fails "late" in the scenario after the turbine pump has been shut down and placed in pull-to-lock; at this point, all secondary cooling would be lost and the operator will need to restart the turbine AFW train or provide some other core cooling

The likelihoods of items 1, 2, and 4 are provided above with the exception that the coincident fire or other serious diversion has not yet been accounted for as part of item 4. Serious diversions could take the form of a significant fire, a coincident pipe breach that causes steam and/or flooding concerns, etc. Considering, for instance, nearly 20 years of nuclear plant experience with approximately 40 fires during that time and a similar estimated number of serious flooding or pipe breach events over the same period, coupled with a current average of approximately 100–200 plant trips per year for the U.S. industry, results in a rough estimate of about one serious diversion event per 50 plant trips or about one per plant lifetime. Hence a 1/50 multiplicative factor needs to be added to the combined likelihood of items 1, 2, and 4. This results in 0.5 per year × 1E-6 × 1/50 = 1E-8 per year.

The probability of the first AFW train failing early or being unavailable can be estimated from current PRA values and is assessed to be about 5% or 5E-2.

The probability of the second AFW train failing to continue to operate can be similarly estimated and, taking into account potential common-cause failure mechanisms between the two trains, is assessed to provide another 5E-2 factor.

Collectively, the above values multiplied together provide an approximation of the frequency of the postulated plant condition of less than 1E-10 per year [1E-8 per year × 5E-2 × 5E-2]. This is considered to be a very unlikely scenario in light of other accident frequencies in the PRA, and probably not worth further consideration.

Frequency of the Entire Event Leading to Core Damage
Considering the above estimate, and even if PSF, HFE, and nonrecovery are now assumed to have probabilities of 1.0 in light of this combination of events, which includes both SG level indicator problems and a distracting event, the expected frequency of such a chain of events proceeding to core damage is assessed as very low since the plant condition has a very low frequency of occurrence.

This observation does suggest the following additional questions: "What if the plant condition involved the loss of all secondary cooling as postulated above, with a serious coincident diversion,

but the SG level indicators were not malfunctioning or otherwise unavailable? Would this be sufficient to divert attention from the lost function and cause the operators to not recover AFW? .

In considering the above change in the chain of events, it should first be recognized that the search process carried out in Step 6 did not suggest that such a scenario would be sufficiently error forcing to cause HFE 2 (i.e., the focus on monitoring SG level would still require the anomalies in these indicators). Further thought simply does not suggest a diversion that is so compelling or threatening that the operators would not monitor the status of the secondary heat sink (a critical safety function) and therefore not notice it had been lost. With the SG level indicators properly tracking the falling SG levels, it is difficult to imagine the operators not restarting the turbine-driven AFW train to recover the lost function. Hence such a chain of events is not judged to be error forcing and therefore is not important.

B.10 Issue Resolution

This illustrative example of the ATHEANA prospective analysis process indicates that while the issue of concern is not among the dominant risk contributors in the plant's PRA, some concern is warranted about conditions that could lead the operating crew to inappropriately cut back or shut down secondary cooling to avoid apparent overcooling concerns. The estimated frequency of such an event progressing to core damage is not so small as to be insignificant. On the other hand, the

likelihood that the operating crew will miss the total loss of secondary cooling because of a serious attention diversion in the plant and thus fail to respond is too small to be considered further.

As for the potential error of commission involving inappropriate cut back or shut down of secondary cooling, a number of "lessons learned" are available which, if enacted, should considerably decrease the chance of such an event. These include:

- discussions with the operating staff as to the results of this analysis and the potential contexts of concern
- training improvements to remove the focus (tunnel vision) on steam generator level indicators as the nearly sole source of heat sink information
- additional procedures and training on the appropriate actions to take when it appears that both MFW and AFW are providing initial feed to the steam generators, thereby creating the tradeoff dilemma raised in this analysis
- fixing the instrument bus–SG level indication interactions so as to avoid the midscale failure mode
- adding simulator exercises to specifically address the concerns raised in this analysis as part of the operating crews' future training

APPENDIX C
ATHEANA EXAMPLE -
LARGE LOSS OF COOLANT ACCIDENT (LLOCA);
A "DIRECT INITIATOR SCENARIO"

This appendix illustrates the use of the ATHEANA process to investigate the potential for operator actions that could seriously degrade plant response to a fast-acting direct initiating event. More specifically, it is an illustration of the use of ATHEANA to identify and quantify those conditions (error-forcing contexts) that may induce unsafe acts by humans. In particular, this example addresses the question: Can physical characteristics associated with the progression of a large loss-of-coolant accident (LLOCA) in a pressurized water reactor (PWR) adversely affect the human operators in ways that have the potential to transform a design basis accident (DBA) into a core damage accident?

This is a plant-specific example, as all fruitful examinations of context must be. However, the plant analyzed is a composite PWR, not exactly matching any particular operating plant. The example is realistic in that all specific design, procedures, training, and operating and maintenance practice information used have been observed in real plants. As a result, this example provides a basis for licensees desiring to investigate similar issues in their plants. The illustration follows the steps discussed in the ATHEANA process in Section 9 of this document.

C.1 Step 1: Define and Interpret the Issue

This ATHEANA example analysis is performed to determine if physical characteristics associated with the progression of a LLOCA initiator can adversely affect the human operators in ways that have the potential to transform a DBA into a core damage accident. The plant PRA identifies the functional failures that lead to core damage.

C.2 Step 2: Define the Scope of the Analysis

In this case, the event type, a LLOCA, is defined by the issue. Characteristics of the LLOCA that are challenging include rapid blowdown, which can lead to uncovery and melting of the core if safety injection or recirculation cooling are interrupted for even a short time. Because of the narrow scope of the issue and the characteristics of the LLOCA, little additional focus on setting priorities should be necessary. However, the question of narrowing the scope must be revisited after identification of the base case LLOCA, the associated human failure events (HFEs), and the search for deviation scenarios.

C.3 Step 3: Describe the Base Case Scenario

The ideal base case, as described in Step 3 of Section 9 and illustrated in the first row of Table C.1, corresponds with a consensus operator model (COM) of the event; i.e., a mental model of the event that operators have developed through training and experience, and that is consistently understood by most operators. Furthermore, it is well defined in both an operational and an engineering sense (thorough neutronics and thermal-hydraulics analysis support the scenario). Finally, it is well documented and realistic. Note that Table C.1 also previews the results of the LLOCA base case development that will be presented in the following paragraphs. For the LLOCA, the base case is very near the ideal case. It will be used as the stepping off point for the deviation analysis. Because the COM is a result of required training based on the DBA, the COM will not be presented separately, but is discussed during the description of the reference case and the base case.

Table C.1 Characteristics of the Base Case Scenario

Type of Base Case	Consensus Operator Model	Well Defined Operationally	Reference Analysis		Realistic
			Well-Defined Physics	Well Documented	
Ideal	Exists	Yes	Matches COM	Yes, public information	Yes
LLOCA base case	Yes; the DBA is well known	Yes; annual training scenario	FSAR DBA closely matches the COM, but the analysis ends after stabilization, but before the long-term scenario is complete	Yes; FSAR	Reasonably realistic; the reference analysis is modified to account for more rapid use of water and long-term issues

C.3.1 The Reference Case LLOCA Scenario

The reference case LLOCA scenario is given in the plant Final Safety Analysis Report (FSAR) Chapter 14 Safety Analysis, Section 14.3.2 Major Reactor Coolant System (RCS) Pipe Ruptures (Loss-of-Coolant Accident), pages 14.3-7 to 14.3-12 plus associated figures and tables in Section 14.3.2.

The LLOCA is a Condition IV limiting fault ("faults which are not expected to take place, but are...the most drastic occurrences which must be designed against...[and] are not to cause a fission product release to the environment resulting in an undue risk to public health and safety in excess of guideline values of 10 CFR 100."). As specified by 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Power Reactors," the FSAR analysis is conservative in many of its details,[1] but the predicted time progression of the major plant parameters is a reasonable representation of the progression of the event. A number of more realistic analyses exist,[2] but are not available in the open literature. Therefore the FSAR case has been selected to define the "reference" case for the analysis.

[1]Conservatisms include break size and location, maximum allowable deviation (drift and error) in actuation setpoints, delay in actuation of safety injection, minimum allowable volumes, minimum heat transfer, maximum initial power, maximum fission product inventory, minimum fuel or clad temperature limits, etc.

[2]Other analyses include the backup document for the Westinghouse Emergency Response Guidelines and various proprietary WCAP thermal-hydraulic reports.

The FSAR analysis assumes a double-ended guillotine rupture of the largest RCS pipe. The FSAR describes the expected sequence of events as follows:

> *Should a major break occur, depressurization of the Reactor Coolant System results in a pressure decrease in the pressurizer. Reactor trip signal occurs when the pressurizer low-pressure trip setpoint is reached. A Safety Injection System signal is actuated when the appropriate setpoint is reached. These countermeasures will limit the consequences of the accident in two ways:*
>
> 1. *Reactor trip and borated water injection complement void formation in causing rapid reduction of power to residual level corresponding to fission product decay heat.*
>
> 2. *Injection of borated water provides heat transfer from core and prevents excessive clad temperatures.*
>
> *At the beginning of the blowdown phase, the entire Reactor Coolant System contains subcooled liquid which transfers heat from the core by forced convection with some fully developed nucleate boiling. After the break develops, the time to departure from nucleate boiling is calculated, consistent with Appendix K of 10 CFR 50 (Reference 1). Thereafter, the core heat transfer is unstable, with both nucleate boiling and film boiling occurring. As the core becomes uncovered, both turbulent and laminar forced convection and radiation are considered as core heat transfer mechanisms.*
>
> *When the Reactor Coolant System pressure falls below 700 psia, the accumulators begin to inject borated water. The conservative assumption is made that accumulator water injected bypasses the core and goes out through the break until the termination of bypass. This conservatism is again consistent with Appendix K of 10 CFR 50.*

The results of the FSAR analysis are shown in Figures C.1 through C.9, where the following points are clearly presented:

- Figure C.1. Power drops almost instantly to about 10%, then decreases more gradually.
- Figure C.2. Break flow (not directly measured and not available to the operators) drops quickly for the first 4 seconds, then more slowly until it bottoms out at about 20 seconds.
- Figure C.3. Core pressure drops smoothly to match containment pressure in about 20 seconds.
- Figure C.4. The containment pressure peaks at less than 20 seconds, as core pressure and break flow approach zero.

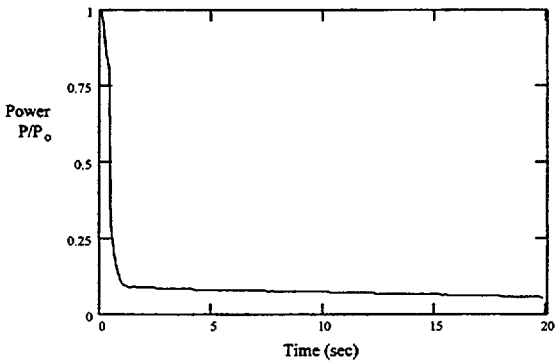


Figure C.1 Core Power during LLOCA Reference Case

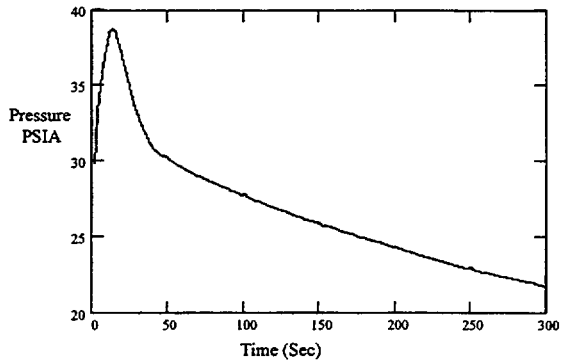


Figure C.4 Containment Pressure during LLOCA Reference Case

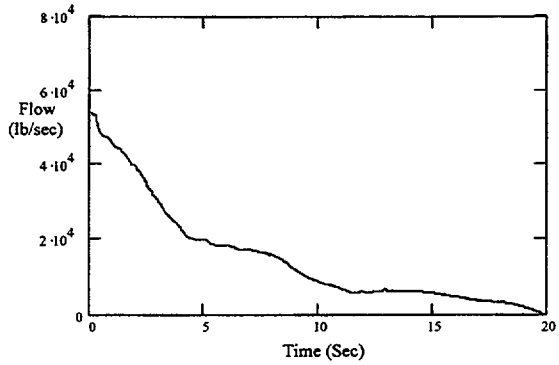


Figure C.2 Break Flow Rate during LLOCA Reference Case

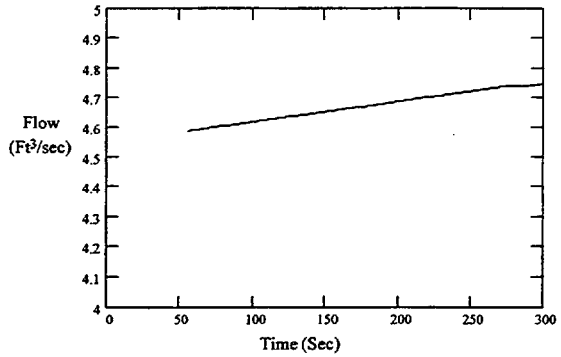


Figure C.5 Safety Injection Flow during LLOCA Reference Case

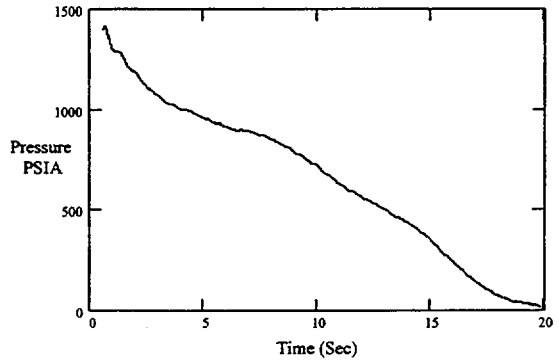


Figure C.3 Core Pressure during LLOCA Reference Case

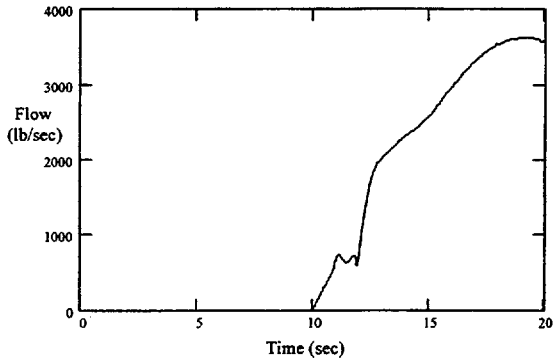


Figure C.6 Accumulator Flow (Blowdown) during LLOCA Reference Case

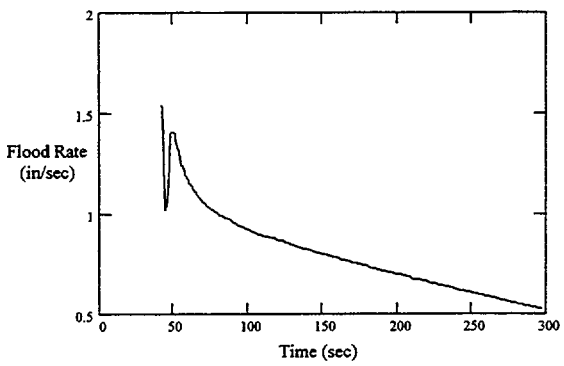


Figure C.7 Reflood Rate during LLOCA Reference Case

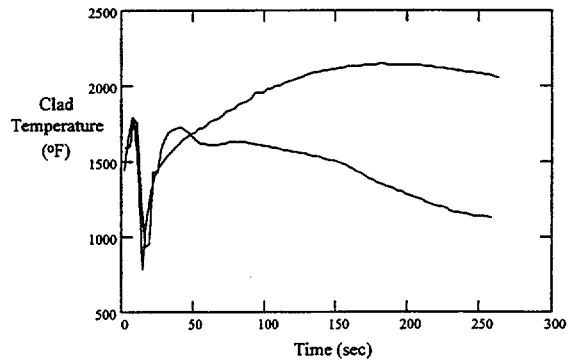


Figure C.9 Peak and Average Clad Temperature during LLOCA Reference Case

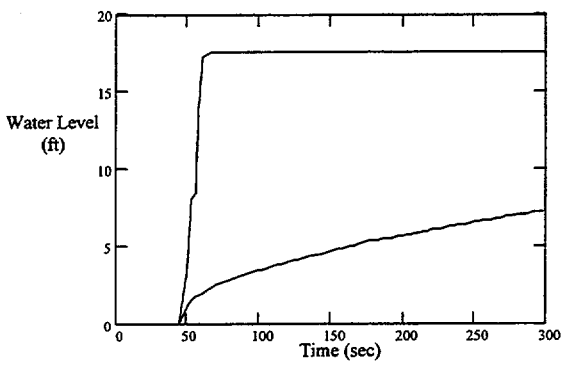


Figure C.8 Reflood Transient Water Level during LLOCA Reference Case

- Figure C.5. Emergency core cooling system (ECCS) flow is credited from about 30 seconds and remains about constant.[3]
- Figure C.6. The accumulators dump into the RCS beginning at 10 seconds and flow peaks at about 19 seconds.
- Figure C.7. Core reflood rate (not directly instrumented) starts at its maximum, when ECCS is assumed to start at 30 seconds. After an initial transient, it decays slowly.

[3]High-pressure ECCS flow would begin almost immediately, while low-pressure flow (about 80% of total flow) would begin as core pressure falls below the shutoff head of the pumps and would reach full flow before 20 seconds.

- Figure C.8. The core is reflooded to 5 feet at about 3 minutes. The reactor vessel downcomer refloods early on. Note that downcomer level is not instrumented and core level [reactor vessel level instrumentation system (RVLIS)] is not calibrated during LLOCA conditions.

- Figure C.9. By about 3 minutes, the most severe effects on the core have peaked, with no core damage.

The key parameters observable to the operators are summarized in Figure C.10. This composite trajectory of the parameters over time constitutes a signature or pattern for the LLOCA, confirmed in reading the FSAR and training materials, and, in the simulator, where the DBA is standard fare.

The reference scenario ends when the core is reflooded and immediate danger to the core is over; i.e., at about 3 minutes. Long-term stability is assumed, as are the operator actions necessary to ensure that stability.

C.3.2 Description of the Base Case LLOCA Scenario

The base case scenario is equivalent to the reference scenario for the LLOCA over the first 3 minutes for several reasons:

- Conservatisms (beyond the initiator itself) in the FSAR analysis of the LLOCA have only minor impact on the sequence of events and parameter changes that occur.

- The view of LLOCA held by operators is guided by their training, which includes the DBA, the double-ended guillotine rupture of the largest RCS pipe of the reference case:

  - operators undergo simulator training on the DBA routinely
  - essentially all operators would define a LLOCA in terms similar to the reference case, i.e., the COM matches the reference case

- Significant variations in the LLOCA, such as break size and location, are not familiar to most operators, except a trained-in belief that the DBA "envelopes" all smaller LOCAs.

The base case scenario, however, extends well beyond the reference scenario in time. The parameters in Figures C.1 through C.9 would return to stable conditions; power continues its gradual decline, core pressure remains essentially flat and equal to containment pressure, break flow (not directly measured and not available to the operators) remains flat at the spill rate and matches injection flow, containment pressure remains flat at near-atmospheric pressure, ECCS flow remains about constant until manual switchover to recirculation cooling at about 20 minutes, accumulator flow continues to fall for several more seconds and becomes zero when accumulator pressure equilibrates with RCS pressure, and core reflood rate (not directly instrumented) continues to decay slowly, reaching zero when the core is completely reflooded. Peak and average clad temperature continue to decrease, approaching the RCS temperature.

Key points in the base case scenario not present in the reference scenario are:

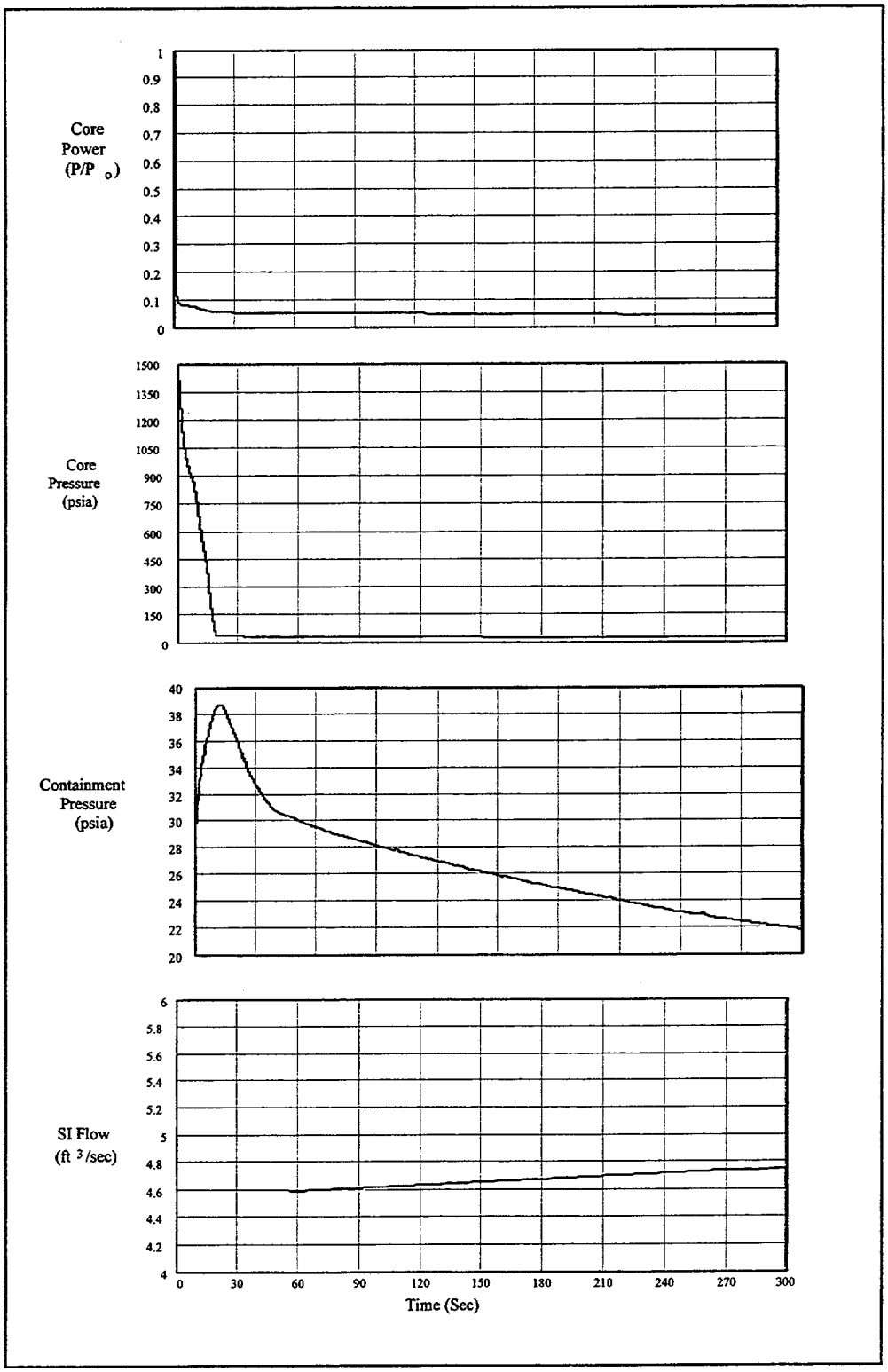


Figure C.10 Observable Parameters during LLOCA Reference Case

- Operators isolate the accumulators after switchover.[4]

- Operators perform the switchover to recirculation cooling after refueling water storage tank (RWST) level reaches 37% [to ensure sufficient emergency sump level to supply the residual heat removal (RHR) pump suction] and must complete the switchover before the pumps lose suction from the RWST (to prevent air binding, pump damage, and starving the core).

- Operators perform switchover from cold leg injection to hot leg injection late in the scenario (to break up any boron crust forming in the reactor vessel, which could interfere with the effectiveness of recirculation cooling)[5]

C.4 Step 4: Define HFEs and/or Unsafe Actions

The LLOCA event tree from the plant IPE is shown in Figure C.11. As shown in the figure, systemic response to the LLOCA (6-inch to double-ended guillotine rupture of the largest cold leg pipe) includes:

- injection of the accumulator water (one of two required)

- low-pressure safety injection [(LPI), one of two RHR pumps to the intact loop]; assumptions: insufficient time for manual recovery, mission time, 1 hour

- low-pressure recirculation cooling [(LP recirculation), one of two trains required]; includes a required operator action

- each sequence ends in success or core damage

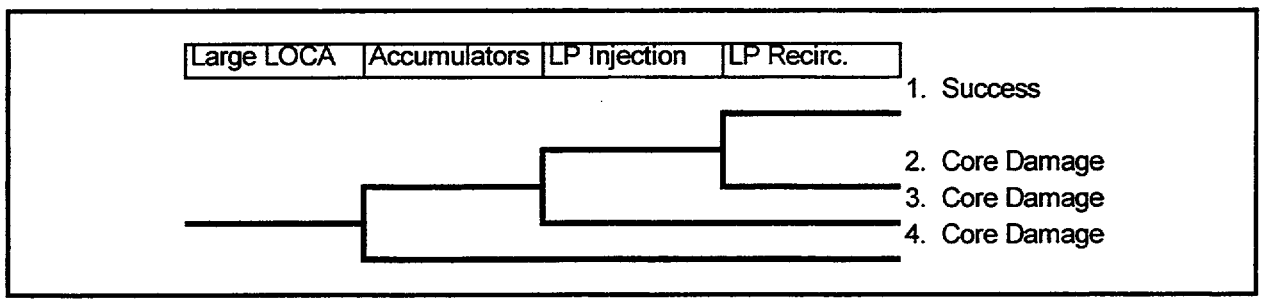


Figure C.11. Large LOCA PRA Event Tree

[4]This step is generally omitted from PRAs because thermal-hydraulic analyses in support of a PRA indicate that nitrogen injection into the loops is not likely to significantly interfere with core heat removal.

[5]This step is generally omitted from PRAs because the best judgment is that boron crust formation is unlikely, except in particular size LOCAs and, even if it forms, can easily be broken up at a later time by shifting to hot leg recirculation.

The ATHEANA process asks that the systemic event tree of the plant PRA be reconstituted as a functional event tree and that other systems and human actions that can provide the same function be identified. For the LLOCA this transformation is quite simple, as shown in Figure C.12. The functions are identified as early makeup (accumulators and low pressure injection, long-term makeup (operators align containment sump recirculation (LP recirculation) at an RWST level of 37% and confirm operation of recirculation cooling), and long term cooling (also provided by LP recirculation, with the cooling function provided by aligning component cooling water (CCW) to the RHR heat exchanger). A reasonable assumption is that the LLOCA progresses so quickly, voiding the core region immediately, that operator action to actuate an initially failed injection system would be ineffective. In addition, because of the stringent requirements of the LLOCA, no other systems than those identified in the PRA event tree are sufficient to provide the same functions.

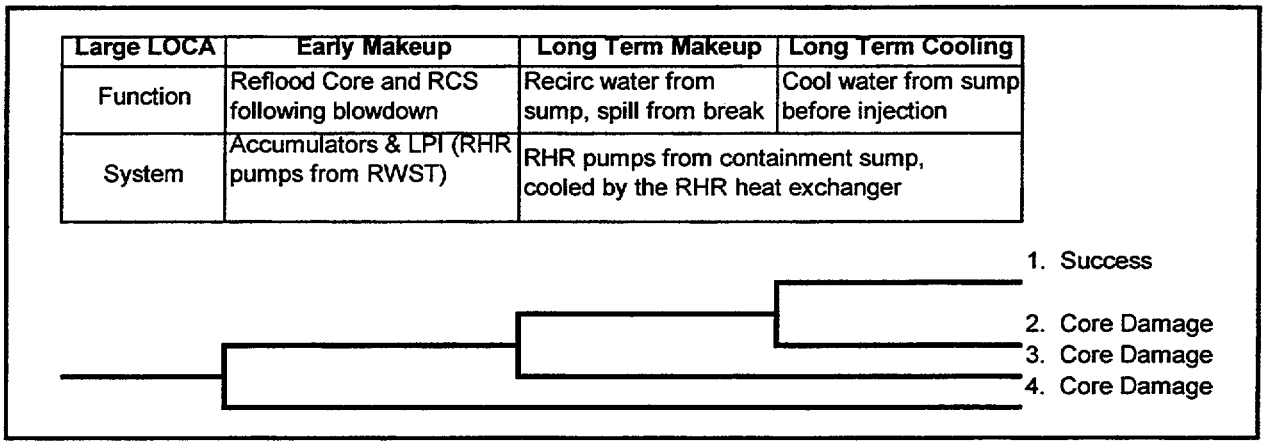


Figure C.12. Large LOCA Functional Event Tree

Application of the HFE identification process (Tables 9.6 and 9.7) leads to the following HFEs:

- Operator improperly removes early makeup from armed or standby status (i.e., improper manual valve lineup blocks accumulator or RHR injection paths, control circuits blocked, or RHR pumps not in auto).
- Operator interrupts early makeup (i.e., operator inappropriately terminates RHR pumps).
- Operator fails to properly align containment sump recirculation cooling.
- Operator prematurely secures long-term makeup or cooling (RHR pumps or CCW to the RHR heat exchangers).
- Operator inappropriately diverts resources (sump water).

All of these HFEs are within the scope of the issue defined in Step 1.

C.5 Identify Potential Vulnerabilities in the Operators' Knowledge Base

To this point, the development and description of the base case LLOCA have been based on thermal-hydraulic calculations for similar events and highlights of the most salient operator actions that are required for successful response to the scenario. A more complete operational view of the LLOCA can be obtained by examining characteristics of the scenario, including information on similarities with training and experience, event timing, identification of operator tendencies, tracking of the emergency operating procedures (EOPs) against the scenario, and identification of informal rules that may affect operator thinking. During this process, we develop information that is helpful in identifying potential vulnerabilities that may make the HFEs more likely than they are under nominal conditions. We post this information on our blackboard for ready access during the search for deviations in Step 6.

C.5.1 Potential Vulnerabilities in Operator Expectations for the Scenario

No operators have ever experienced a LLOCA scenario at a U.S. PWR. However, all PWR operators receive regular training on the DBA LLOCA of the base case scenario. Therefore their expectations are very strongly aligned with the base case. However, few operators receive training on smaller LLOCAs (including those called "intermediate LOCAs" in the PRA), so deviations of this sort will be outside of their training and experience. Rules (formal and informal) may not conform with scenarios that deviate from the base case.

Despite extensive training and the clarity of symptoms of this direct initiator, the base case LLOCA is a severe event that no operator expects to see in a real plant. Disbelief may be strong, despite training.

C.5.2 Time Frames for the LLOCA

From the FSAR analysis in Step 3 and the discussion of the base case scenario, five distinct time periods can be identified. These are listed in Table C.2, along with a note of the potential for operator influence.

By the end of the second time frame, 0-20 seconds, the LLOCA blowdown is complete; i.e., the LOCA has ended. By the end of the third time frame, the potential for immediate damage is over; i.e., the LOCA and its direct consequences are finished, without damage to the core. All that remains is the long-term control of stable conditions. Note, however, that the operators have a number of important activities remaining, especially switchover to recirculation cooling at about 20 minutes.

Table C.2 Time Frames for the Base Case Large LOCA

Time Frame	Occurrences	Influences on/by Operators
Initial conditions	Steady state, 100% power No previous dependent events in base case	Routine conditions; nothing to focus attention
Initiator/simultaneous events	Reactor power prompt drop Pressure drops below SI initiation point	These events are over before the operator even recognizes what is happening
Early equipment initiation and operator response: 0-20 seconds	Break flow is complete Pressure drops to essentially zero Containment pressure has peaked and is falling ECCS flow begins Accumulator flow occurs	During this time frame the operator is checking parameters and ensuring appropriate standby equipment has started. Some early decisions in the EOPs may have occurred
Stabilization phase 1-3 minutes	Core reflood begins at about 30 seconds and has reached stable conditions Fuel temperatures have peaked and are falling	During this time, the operators have moved into the LOCA EOP and have passed a number of decision points
Long-term equipment and operator response	Isolation of the accumulators Shift to cold leg recirculation cooling Shift to hot leg recirculation cooling Repair and recovery	During the 20 minutes until switchover to cold leg recirculation cooling, the operators are occupied with confirmatory steps in the EOPs. Any complications beyond the base case scenarios can affect their performance This longer time frame extends to days and months. There are no critical operations concerned with the base case scenario. Problems during this phase would be the concern of a low power and shutdown PRA.

C.5.3 Operator Tendencies and Informal Rules

Of the operator tendencies presented in Table 9.12a of the ATHEANA process, most factors in the LLOCA base case scenario induce appropriate tendencies to control the scenario. For example, low pressurizer level and pressure induce the appropriate tendency to increase injection. They also point toward isolating LOCA paths, decreasing letdown, and turning on pressurizer heaters. However, the heaters would not be helpful for the LLOCA because the pressurizer would be empty. In fact, if the heaters were actuated and not protected by low-level control circuits, they would burn out, which could attract attention and cause some confusion. Finally, high core heat removal (here due to the LOCA blowdown) would in itself encourage undesirable tendencies to decrease injection. It would also create a tendency to decrease RCS forced flow. High containment pressure and temperature would encourage containment isolation, cooling, and spray, all useful tendencies.

A number of informal rules and practices that operators in this plant tend to observe could affect the base case LLOCA and deviations from it. A generic list of informal rules was provided in Table 9.13 of the process and, using the table to guide our thinking, we have evaluated these rules on a plant-specific basis. We have also evaluated plant-specific practices. The results follow:

- Protect equipment. A recent history of running two balance-of-plant pumps to destruction through cavitation and overheating has made operators acutely aware of the hazards of operating pumps with insufficient net positive suction head (NPSH) and dead-headed. Vibration noise is one of the factors they are most sensitive to.
- Recent history of performance. A series of recent problems with the channel A pressurizer pressure instrument has made operators suspicious of its performance. They tend to follow channel B, rather than auctioneered pressure.
- Crew characterization. Formal communication, strong shift supervisors (lower watch standers seldom question supervisor's judgments), low tolerance for perceived gaps in knowledge.
- Lack of deep technical knowledge. Few shift operators have deep understanding of instrument sensor design and the algorithms used in the I&C circuits. Instrument technicians are available during the day shift and can be contacted or recalled on back shifts.

Step 6 will investigate potentially negative impacts of these tendencies and informal rules in the face of deviations from the base case or other complicating factors.

C.5.4 Evaluation of Formal Rules and Emergency Operating Procedures

Perhaps the best operational view of the scenario can be developed by tracking those elements of the EOPs that are processed in the LLOCA. A map of these procedures is provided in Figure C.13 (shown at the end of this chapter because of its large size). The expected procedural pathway for the base case LLOCA is shown by solid arrows. The procedure map tracks all key decision points in the EOPs: (a) branch points to other procedures, (b) internal steps that disable plant functions (i.e., stopping particular plant components that can supply functions that are sometimes needed), and (c) steps that require a major reconfiguration of equipment. Figure C.13 (located at the end of this appendix) combines all procedures carried out during the base case LLOCA scenario. At each decision point (e.g., E-1, Step 2 in Figure C.13), a table in the figure provides the following information:

- actions to be taken
- the potential for ambiguity in the decision criteria in the base case
- a judgment on the significance of taking the wrong branch or inappropriate action

All steps that disable plant functions are indicated by hexagonal boxes (e.g., E-0, Step 20 in Figure C.13). This information is expanded to support the deviation search process by indicating deviation classes under which ambiguity is increased and changes in the significance of taking wrong branches due to effects of possible deviations. For cases where the significance could be high, the box is **bold** and the key aspects of the significance are shown in ***bold italics***. For those cases, relevant potential

ambiguity is also shown in ***bold italics***. The examples cited above show these characteristics. This information will be used later in Step 6, in combination with information concerning informal rules and operator tendencies, to help insure that the consideration of deviations includes identifiable "bad actors."

The path through the procedures for the base case LLOCA is very clear and unambiguous. Taking wrong branches that preclude being alert for early switchover to recirculation cooling (i.e., any path off the LLOCA path) could have serious consequences because the time available for switchover is short and failure will lead directly to core damage.

In addition to the Figure C.13 information, the EOPs provide for continuous monitoring of critical safety functions. EOP F-0.6, inventory, is the earliest indicator of problems and requires monitoring of the following:

- Pressurizer level (>19%)
- RVLIS (void fraction % stable or decreasing or reactor coolant pumps (RCPs) A and B OFF ≥100%)

Depending on the outcomes of these decisions, other function recovery procedures may need to be implemented if additional complications occur during the scenario. These procedures ensure that operators are reminded that injection is required if pressurizer level is low. If the level is high, steps are recommended to compress voids.

C.5.5 Summary of Potential Vulnerabilities

At the close of Step 5, we have posted the information collected on training and experience, time frames, operator tendencies and informal rules, and the EOP map on our blackboard and are ready to begin a systematic search for deviations from the base case scenario in Step 6. Before moving ahead with the search, it will be helpful to summarize the most interesting potential vulnerabilities uncovered during Step 5. That summary is presented in Table C.3.

C.6 Step 6: Search for Deviations from the Base Case Scenario

This search is structured to identify key elements of plant conditions and some aspects of performance-shaping factors that can be primary elements of error-forcing contexts for scenarios that deviate from the base case LLOCA. The resultant error-forcing context (EFC) elements will be refined in later steps of the process. Up to this point in the analysis, the process has been straightforward, proceeding in a well-defined, step-by-step progression. However, the searches described in Step 6 of Section 9, while structured, involve substantial iteration, free-wheeling exploration, and intuitive integration.

Table C.3 Summary of Potential Vulnerabilities for LLOCA

Consideration	Observation	Vulnerability or implication
Training and experience	LLOCA has never happened; seems impossible	Disbelief
	Annual DBA training	Expectations aligned with base case; similarity bias
	No training or experience on LLOCAs<DBA	Unfamiliar, therefore weak knowledge; must adapt DBA
Time frames	LLOCA stabilized by 3 minutes	Intervention during this time period, while unlikely, could be serious
	RWST low level at 20 minutes, recirculation cooling required	Short time available to effect switchover
Operator tendencies	Tendencies: most are appropriate and helpful. However, the tendency for high core heat removal is to decrease injection	Taken alone, overcooling implies reduced injection flow
Informal rules	Pumps will be damaged by low NPSH and deadheading	Strong tendency to stop pumps with suspected vibration noise
	History of channel A pressurizer pressure problems	Believe channel B
	Crew follows formal communication practice, with very strong shift supervisors	Low tolerance of knowledge gaps Lower-level watch standers are hesitant to question shift supervisors
	Lack of deep technical knowledge of I&C, especially instrument and sensor design, and physics algorithms. No technicians on back shifts.	Operator confusion is likely if deviations from base case operations require detailed knowledge of I&C systems
Formal rules/EOPs	No significant ambiguities identified for the base case. A number of steps with high potential significance were identified, which could become ambiguous, depending on the deviation from the base case.	See Figure C.13 for details. Potentially significant consequences can be found at: E-0, Steps 3, 4, and 20 E-1, Steps 1, 2, 12, 14, and 16-19.

Caveat: The analyst new to ATHEANA must resist being fooled by the stepwise presentation of the search in the following paragraphs. What you are about to read is the result of many trials, dead ends, and misdirections. As described in Section 7, the ATHEANA analysis requires a broad range of multidiscliplinary knowledge: behavioral and cognitive science, the plant-specific design and

PRA, understanding of plant behavior (including thermal-hydraulic performance), understanding of the plant's operational practices (including procedures, training, and administrative practices), and generic and plant-specific operating history (including incident history, backlog of corrective maintenance work orders, and current workarounds). The analysts bring this catalog of knowledge to bear, along with the blackboard full of information collected in Step 5, to find the most significant deviation cases. The mental process that allows this integration is complex, not well understood, and not well suited to a step-by-step description, just as the view of a chess game by an expert is more complex and effective than a brute-force lookahead computer program. The process requires a strong facilitator or integrator, who has broad general knowledge of all the disciplines and can challenge any other experts involved in the process. Finally, even if a single analyst can bring all the requisite knowledge to the table, it is essential that others be involved to challenge assumptions, shortcuts, and possibly overly narrow analysis.

C.6.1 Search for Initiator and Scenario Progression Deviations from the Base Case Scenario

This search proceeds in the manner of a hazard and operability analysis by applying the series of guide words introduced in the process description to the base case LLOCA scenario. For each guide word, we seek physical changes associated with the initiating event that could enable the plant behavior described by the guide word. [Scenarios can also deviate from the base case because indicators (instruments) follow the guide word, while the scenario is otherwise undisturbed until the control systems or operators intercede; as a result of the deviation in instrument response. Such situations are reserved for Step 7, where other complicating factors are considered.]

Using Section 9.6.3 of the process description, the first guide word we apply is "no or not." The idea is that the guide words trigger the imagination of the analyst to identify potentially significant scenarios. There is no concern that the guide words be independent and no effort should be wasted worrying whether a particular deviation case should be categorized under one guide word or another. The guide words are not tools for categorization, but stimulants to the imagination.

What does it mean for there to be "no" LLOCA? It can mean that the loss of coolant itself is less than that assumed in the DBA of the base case. It can also mean that some physical parameters of the plant behave as if the LLOCA were smaller.

"No" LLOCA Deviation Case (<DBA). The LLOCA can be smaller than the base case if the break size in the RCS is smaller than the large double-ended guillotine break of the cold leg; e.g., a break nearer the 6-inch lower size of the PRA's LLOCA. Breaks of this size would offer a variety of challenges to the operator. First and most importantly, breaks of this size (well above the 2 inch size of the small LOCA (SLOCA), but much smaller than the DBA) are not analyzed in the FSAR safety analysis and are generally not discussed in training or exercised on the simulator. Therefore, the operators will not be familiar with the timing and exact sequencing of events. Figure C.14 sketches the kinds of change in parameter trajectories associated with this deviation. Depressurization occurs more slowly and would substantially extend the time until switchover if containment spray (CS) did not rapidly deplete the RWST. Note that while the scenario takes longer to evolve than the base case

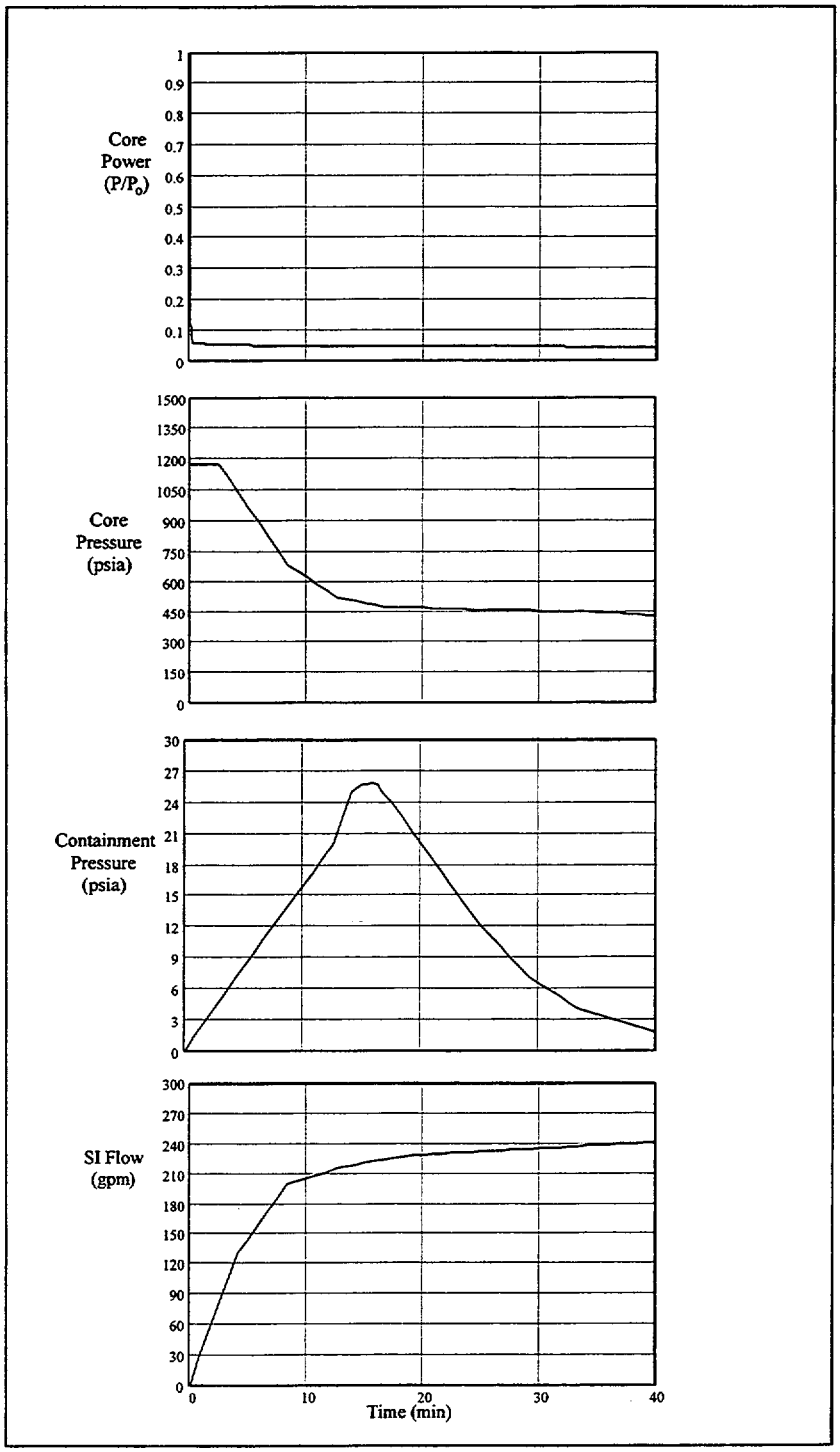


Figure C.14 Observable Parameters during "No" LLOCA Deviation (<DBA) Case

LLOCA, it is substantially faster than an SLOCA. If the operator is thinking SLOCA, the time to switchover could come quickly and the time available for switchover will be significantly reduced. Breaks of this size, while very unlikely, must be more likely than the base case LLOCA (DBA).

To begin the evaluation of this deviation case, we play the scenario against the EOPs, as represented in the map of Figure C.13. Walking through the EOPs, with the timing of Figure C.14 in mind, shows first of all that the procedure works; i.e., it is technically correct. However, differences in timing with respect to two familiar cases (the base case LLOCA and the FSAR small LOCA) have the potential to make some of the ambiguities raised in Section C.5 more significant. Specifically, with no further complicating context, the operators are expected to have no problems due to the deviation in E-0 and should successfully transition to E-1. In E-1 all should go smoothly and at step 18 RCS pressure will be >150 psig, so the operators should transition to ES-1.2. Because the base case did not make this transition, ES-1.2 is mapped separately in Figure C.15, which is also shown at the end of this appendix.

Continuing in ES-1.2, first note that incorrect decisions at several steps in ES-1.2 can increase the size of the LOCA, especially if RCP seal cooling has been lost. Such changes, while not a major effect, could create confusion. Next, a warning is provided at depressurization steps 9 and 14 that voiding can occur in the RCS that would cause rapidly increasing pressurizer (Pzr) level (the TMI scenario). In addition to the warning, the procedure progresses in stepwise fashion to limit the chance of voiding, by keeping control of the RCS level and subcooling. Nevertheless, if the context becomes sufficiently challenging beyond the deviation scenario condition, old rules can be enabled, such as the "Don't go solid" informal rule. Finally, the SI pump stop criteria in step 11.d, while familiar from SLOCA simulator drills, is fairly complex and takes time to follow correctly. It directly controls high pressure injection and therefore level, pressure and subcooling. Errors in this step can lead the operators on an unnecessary cycle through the procedure, during which time conditions can be degrading due to an incorrect action. Transfer to sump recirculation could be delayed because of a belief that transfer to RHR cooling will occur soon. In addition to all this, the goal of ES-1.2 is to place the RCS on long term RHR cooling or to reach a stable leak and fill condition using the charging pump for makeup. If the emergency director does not choose to place RHR in service in step 24.c (e.g., because of concerns about residual steam in the RCS binding RHR flow) and the LOCA is greater than the capacity of the charging pump, the only procedural path to sump recirculation cooling is via the E-1 "Foldout Sheet."

Two of the HFEs identified in ATHEANA Step 4 could be enabled, but are not likely without further and sufficiently challenging context (note that the "No" LLOCA deviation case slightly changes one of them):

- Operator interrupts early makeup
- Operator fails to properly align containment sump recirculation cooling or RHR

Returning to the vulnerabilities summarized in Table C.3, we observe that:

- training and experience are weak for this deviation case

- the operator tendency to reduce injection for overcooling is very unlikely to have any impact, unless something causes them to fixate on temperature alone (a massive instrument problem would be required to miss the strong indications of LOCA)

- the history of channel A Pzr pressure problems would be unimportant without failure or erroneous indication on channel B

At this point, the possible physical deviation is well-defined and has been determined to be important enough to proceed to the next part of the analysis. The results of the application of the guide word "No" to the LLOCA base case are summarized in Table C.4, which comes at the end of the guide word analysis of this section. What remains is to look more formally at the human behavior factors affecting performance to see if the conditions presented are likely to be significantly challenging to plant operators.

Next the deviation scenario is examined for challenging context against the scenario descriptions and parameter characteristics listed in Tables 9.15 and 9.16. As explained in Section 9.6.3 of the process description, these tables provide a link between observable scenario/parameter characteristics and error types and error mechanisms (and information processing stages) of behavioral science. Based on the scenario analysis above and information in the tables, we find that the "No" LLOCA (< DBA) case involves at least five different, potentially troublesome characteristics:

- Large change in parameter; under the deviation scenario, this can affect situation assessment and response planning. In itself, this may have minor impact. The change is well within the range observed in training scenarios.

- Low rate of change in parameter compared with the base case LLOCA; can affect situation assessment and response planning.

- Relative rate of change in two or more parameters is not what would have been expected; can affect situation assessment.

- Changes in two or more parameters in a short time; can affect situation assessment.

- Direction of change in parameters over time is not what would be expected; can affect situation assessment. The situation is outside of operator training and, therefore, the operators' mental model.

All these human complications would spell difficulty for the operator and could support the two HFEs listed above, except that the procedure can guide them through it successfully. It is likely that additional factors are needed, such as those identified as causing increased ambiguity in the EOP discussion above, for this to become a significant EFC. For example, lack of crew discussion of confusing situations (informal rules and practices) could compound any misdirection.

The other class of "No" LLOCA scenarios that deviate from the base case LLOCA involve physical parameters of the plant behaving as if the LLOCA were smaller. Parameters identified in the reference case included:

- *Power.* It could fail to drop on LLOCA, if it were over-moderated because of a fuel load error or a violation of control rod program management. This is certainly outside the range of training and operator mental models and could result from human unsafe acts. For now we assume that the probability of such events is low compared to other possible contributors, but it might be worth pursuing at a later date.

- *Pressure.* No phenomenological reason for delayed pressure drop has been identified.

- *Break flow.* No phenomenological reason other than actual smaller LLOCA for lower break flow has been identified.

- *Containment pressure.* The impact of passive heat sinks in the containment could significantly delay pressure rise and peak values. No important impact on operator performance has been postulated.

- *ECCS flow.* ECCS flow can be blocked because of pump or valve failure and these cases are modeled in the PRA. Such failures could be due to a previous HFE in which the operator improperly removed the equipment from the armed/standby status. Given the plant surveillance process, such a situation is very unlikely (although it happened at TMI). It is eliminated from consideration in this analysis, because it is outside the scope of the issue defined in Step 1, limiting the question to the impacts of *physical characteristics* associated with the LLOCA progression. Under other issues, this case may be worthy of pursuit.

  "Less" ECCS flow can occur, because of obstructions or impaired pump performance, or because a smaller LLOCA has occurred and pressure remains too high for full RHR pump flow. The smaller (< DBA) LLOCA scenario was analyzed earlier. The actual impaired flow scenario falls naturally into two cases: those in which flow is reduced below that required to survive the initiator (this case is modeled in the PRA systems analysis) and those where it is sufficient for long term success, but decidedly less than expected and, perhaps, less than needed to meet design criteria early on. Such a case would involve delayed core reflood (not observable to the operator), possible fuel damage resulting in high fission products in the RCS, and, possibly, delayed switchover to sump cooling. Of these, the only one that is likely to be observed and of concern to the operator would be the high fission product concentration in the coolant. It is difficult to see how this would cause significant problems to the operator other than minor confusion and concern, unless this extra burden intensified the pressure due to other outside EFC.

- *Accumulator dump.* Improper nitrogen pressure on the accumulators would delay or speed up their discharge, with little anticipated impact on the accident progression or, therefore, on operator response. From thermal-hydraulic analyses of LOCAs with and without accumulator discharge, impact of such problems on operator performance seems unlikely.

- *Core reflood rate and timing.* No phenomenological reason for delayed reflood has been identified, other than reduced ECCS flow described above..

- *Clad temperature.* No phenomenological reason for decreased clad temperature has been identified.

When we applied the other negative guide words ("Less," "Late/Never," "Too slow," "Too long," and "Part of"), we found that all lead the analysis to the same result. In this example, "No" is a surrogate for all these other words.

"More" LLOCA Deviation Case. The next guide word to consider is "More" (or "Early," "Too quick," or "Too short"). This requires a break size greater than the DBA (i.e., severing of two or more loops or fracture of the reactor vessel), which is very unlikely except under seismic excitation well beyond design or if PTS occurs to a vulnerable vessel. Plant-specific information for this reactor vessel indicates that it is not particularly vulnerable to PTS rupture. At this time, we believe such an event is so low in frequency as to be negligible with respect to risk. We note, however, that while the PRA assumes core melt is guaranteed under such conditions, it is possible to survive some LLOCAs beyond the DBA if all injection systems work. The plant is designed to survive the DBA with any single active failure, e.g., failure of an RHR (LPI) pump. HRA of such an event (after thermal-hydraulic success criteria have been determined) would be concerned with a shortened time to switchover and a reduced time available for switchover. This scenario would be outside of the operators' training and indications that an event greater than the DBA would probably not be recognized.

"Reversed" LLOCA Deviation Case. The next guide word is "Reversed." The notion appears to be meaningless for the LLOCA.

"As Well As" LLOCA Deviation Case. Finally consider "As well as," which also includes "Repeated" and "Inadvertent." Here the idea that developed is that the initial LLOCA suddenly becomes blocked (e.g., by RCS internals that have come loose). An event of this sort could start a bit confused, but quickly appear to be an SLOCA. The observable parameters are sketched in Figure C.16, where a very unfamiliar pattern is seen. Containment pressure looks like a LLOCA. RCS pressure initially falls like a LLOCA, but quickly begins to recover, which is almost surely an unexplainable time history for the operators. Safety injection (SI) flow begins high, but quickly drops to SLOCA levels, when pressure rises above the shutoff head of the RHR pumps. These early, inconsistent details are likely to be ignored as the reality of the SLOCA sets in. Soon, SI pumps will be stopped and the system stabilized. When the debris vibrate loose, reestablishing the LLOCA, there will be little time to recognize what has happened and reestablish full SI, before core damage occurs. This is certainly an unfamiliar scenario. Fortunately it is very unlikely. Nevertheless, we pursue it further because of its unique and potentially challenging characteristics, until it can be proved to be impossible. We also note that a similar scenario would involve a small LOCA that appears to stabilize and later expands quickly to a near DBA LLOCA. Such a scenario would not be as confusing, lacking the unexplained beginning, but could lead to an identical situation. We will call this deviation case the "Switching" LLOCA, being a special case of "as well as."

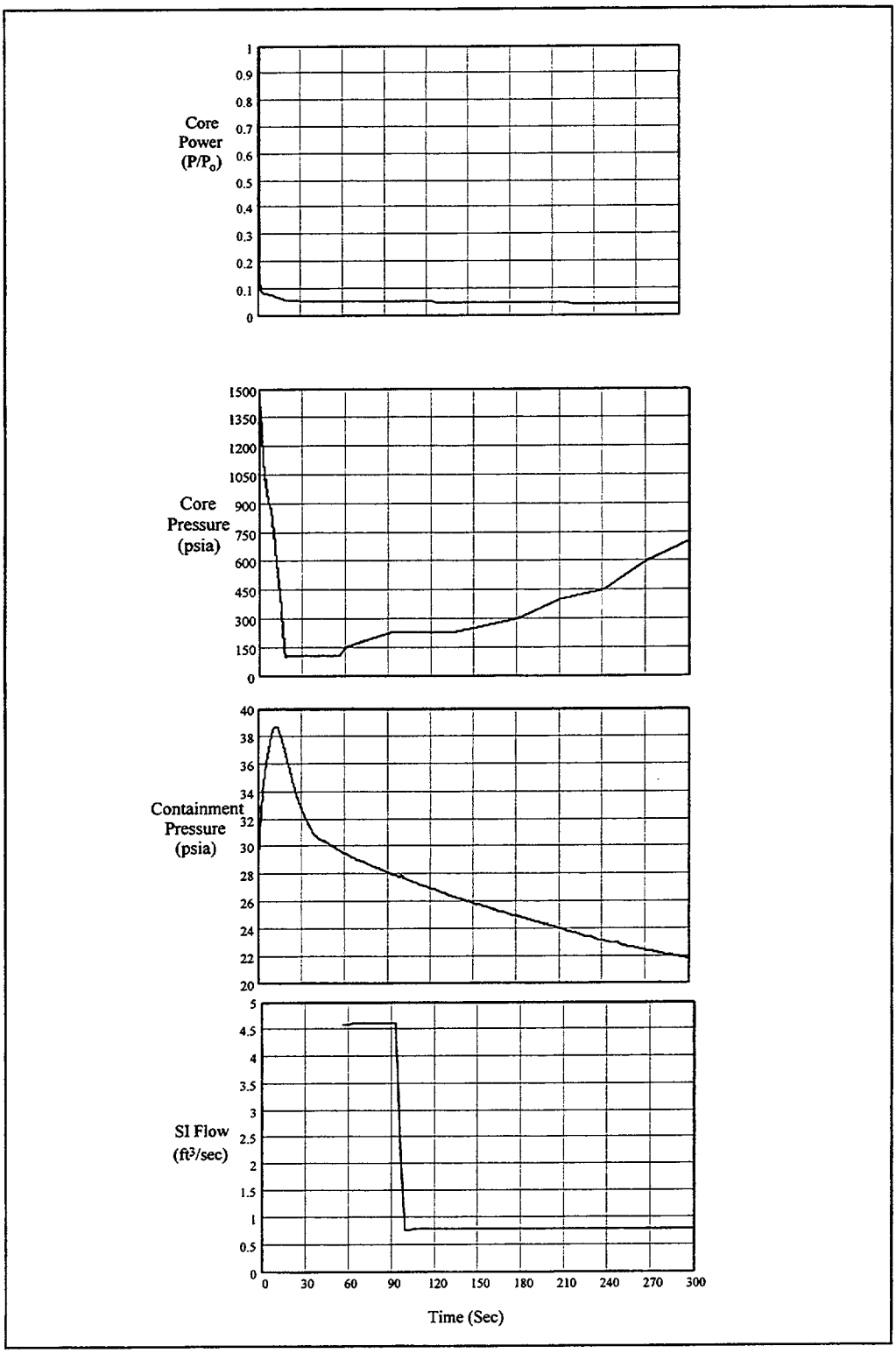


Figure C.16 Observable Parameters during LLOCA "Switching" Deviation Case

Let us take a closer look by tracking the "Switching" LLOCA scenario through the EOPs. Again we begin with the base case LLOCA procedure map of Figure C.13. The early plant response (large drop in pressure and temperature, combined with very high containment pressure) would carry the operators through the initial stages of E-0 with little question. By step 18 some questions and uncertainty could arise. Temperature will be well below 547F and, depending on when they reach this step, it will either be continuing to fall or trending back up. For a LLOCA, temperature would be falling and operators would expect to be securing steam dump. (For an SLOCA they would have expected to need to dump steam and that certainly is not the case.) If they notice the increasing pressure and limited injection flow, they might begin to suspect a steam or feed rupture inside containment. In any case, faith in the diagnostic power of E-0 will still be strong. At step 21, they should find no need to transfer to E-2, the faulted steam generator (SG) isolation procedure, as all SGs should look the same. Even if they choose the wrong path due to a strong belief that a steam break must be the problem, E-2 will send them to E-1, loss of reactor or secondary coolant, with only a slight delay, after isolating the SGs. The loss of secondary heat sink could become a problem later, but not at this time.

In E-1 all should go smoothly initially. At step 14, just before securing the RHR pumps (a different path through the EOP than the base case), the operators are cautioned that "If RCS pressure decreases in uncontrolled manner below 150 psig, RHR pumps must be manually restarted to makeup the RCS." This is an important warning for the "Switching" LLOCA scenario, but we note that there is no other caution or check for this condition other than the critical safety function status tree for core cooling, which looks at the core exit thermocouple readings at irregular intervals. The caution is not on the E-1 foldout sheet, which would be available as a ready reminder. When the LOCA grows sometime later, the crew will be involved in wrapping up the stable and supposedly well understood SLOCA. For now, the crew continues with E-1 until step 18 where, because RCS pressure is above 150 psig, they should transition to procedure ES-1.2, post LOCA cooldown and depressurization. This is the same path followed by the "No" LLOCA case and we can follow the same map of ES-1.2 in Figure C.15.

Continuing in ES-1.2, first note that incorrect decisions at several steps in ES-1.2 can increase the size of the LOCA, especially if RCP seal cooling has been lost. Such changes, while not a major effect, could add to confusion. The next real trap for the "Switching" LLOCA case comes in step 3.e where, in the first cycle through steps 3-26, the operators are again asked to stop RHR pumps, which will leave the plant with insufficient injection, when the LLOCA begins again. Note that this is not an error. If the pumps are not stopped they will be damaged due to lack of flow. It is, however, an act that leaves the plant vulnerable. Failure to closely monitor pressure, while in a vulnerable state (i.e., until fully depressurized) would be a significant unsafe act.

After step 6, they may not have recovered subcooling, so the EOP path may move on to step 7, rather than step 16, as shown. Next, a warning is provided at depressurization steps 9 and 14 that voiding can occur in the RCS that would cause rapidly increasing Pzr level (the TMI scenario). In addition to the warning, the procedure progresses in stepwise fashion to limit the chance of voiding, by keeping control of the RCS level and subcooling. Nevertheless, if the context becomes sufficiently challenging, old rules can be enabled, such as the "Don't go solid" informal rule. Finally, the SI

pump stop criteria in step 11.d, while familiar from SLOCA simulator drills, is fairly complex and takes time to follow correctly. It directly controls high pressure injection and therefore level, pressure and subcooling. Errors in this step can lead the operators on an unnecessary cycle through the procedure, during which time conditions can be degrading due to an incorrect action. Transfer to sump recirculation could be delayed because of the belief that transfer to RHR cooling will occur soon. (Furthermore, if the LLOCA reoccurs during step 11.d, the careful focus on the step by step rules in the EOP, especially as conditions are changing, could involve a type of "tunnel vision," delaying recognition that a LLOCA was again in progress.)

The goal of ES-1.2 is to place the RCS on long term RHR cooling or to reach a stable leak and fill condition using the charging pump for makeup. If the Emergency Director does not choose to place RHR in service in step 24.c (e.g., because of concerns about residual steam in the RCS binding RHR flow or the odd, unexplained conditions at the beginning of the scenario) and the LOCA is greater than the capacity of the charging pump, the only procedural path to sump recirculation cooling is via the E-1 "Foldout Sheet."

Once the LLOCA is re-established and, if the operators spot it in time to start the RHR pumps and save the core, it is fair to question how they would use the EOPs. They could jump back to E-0 or E-1. The case is formally included in the EOPs as cautions in E-1, Step 14, and ES-1.2, Step 3. Thus the operators could return to one of those points or carry out the action to start the RHR pumps and continue cycling through ES-1.2, Steps 3-26. The first would naturally take them to sump recirculation cooling in Step 19, if they reach that step in time. The second would simply cycle unsuccessfully hoping to refill the Pzr, when we really should not be in this procedure because we do not meet the >150 psig criterion to enter it. The E-1 foldout, still in effect formally would transfer to ES-1.3 sump recirculation.

From this discussion, it appears that, while the EOP can work for the "Switching" LLOCA deviation case, there may be some rough spots for the crew. Along the way several actions listed as HFEs in ATHEANA Step 4 could be enabled by this deviation scenario:

- Operator removes early makeup from armed/standby status. (Note that this action to disable the RHR pumps is required by the EOP to protect the pumps and is not, therefore, an HFE. It does, however, defeat automatic response of the pumps if they are subsequently needed.)

- Operator fails to properly align containment sump recirculation cooling. (This HFE would be enabled simply by the cyclic structure of ES-1.2, and would be reinforced by the "Switching" LLOCA, because of the differences in timing introduced by a LLOCA occurring after the RWST is partially depleted by the preceding SLOCA.

- Operator fails to manually start RHR pumps, when required. (This is a new HFE, not identified for the base case LLOCA, in ATHEANA Step 4—one that is introduced due to the "Switching" LLOCA deviation scenario.)

Returning to the vulnerabilities summarized in Table C.3, we observe that:

- training and experience do not directly apply; they apply to either the LLOCA or SLOCA base case, but the "Switching" deviation introduces problems in recognition, timing, and EOP ordering

- the operator tendency to reduce injection for overcooling is very unlikely to have any impact

- the history of channel A Pzr pressure problems would be unimportant without failure or erroneous indication on channel B

- the informal rule to protect pumps from damage would reinforce the procedural stopping of RHR pumps and tend to place the focus on protecting the pumps rather than being alert to their future need

At this point, the possible physical deviation is well-defined and appears to be important enough to proceed to the next part of the analysis. It is time to look more formally at the human behavior factors affecting performance to see if the conditions presented are likely to be significantly challenging to plant operators.

The "Switching" LLOCA deviation scenario is examined for challenging context against the scenario descriptions and parameter characteristics listed in Tables 9-15 and 9-16. As explained in Section 9.6.3 of the process description, these tables provide a link between observable scenario/parameter characteristics and error types and error mechanisms (and information processing stages) of behavioral science. Based on the scenario analysis above and information in the tables, we find that this case involves at least eight different, potentially troublesome characteristics. This is not surprising; we are involved in a significant deviation from expected plant conditions outside the training and expectations of the crew. This is just the kind of situation implicated in serious accidents in which the operators are "set up" for failure. The identified scenario/parameter characteristics include"

- Large (initial) change in parameter; under the deviation scenario this can affect situation assessment and response planning. In itself, this may have minor impact. The change is well within the range observed in training scenarios.

- Low rate of change in parameter; can affect detection, situation assessment and response planning.

- Relative rate of change in two or more parameters is not what would have been expected; can affect situation assessment.

- Changes in two or more parameters in a short time (following a period of stability); can affect detection and situation assessment.

- Garden path problem; can affect situation assessment.
- Situations that change; can affect situation assessment.
- Multiple lines of reasoning; can affect situation assessment.

These human complications spell difficulty for the operator and support the three HFEs listed above. Although the procedure can guide them through it successfully, there are significant factors that can defeat its success.

Summary of Deviation Cases. Results of the preceding guide word deviation analysis are summarized in Table C.4, where, for each guide word, we summarize the identified possible physical deviations and their significance. We also indicate which of these deviation cases are considered further. The summary analysis is continued in Table C.5, where the scenario/parameter characteristics of the deviation cases from Tables 9.15 and 9.16 are presented. The analysis of these characteristics is extended in the table by identifying the associated error types and error mechanisms from Tables 9.15 and 9.16 that apply to each deviation case.

Consider the "No" LLOCA deviation case. Despite the large number of error types and error mechanisms that could enable the two HFEs

- Operator interrupts early makeup
- Operator fails to properly align containment sump recirculation cooling or RHR

there is substantial time for the operators to respond to the many directions in the EOPs that would restore the scenario to a success path. It appears that the "No" LLOCA deviation case surely requires additional error-forcing context (e.g., instrumentation problems or significant extraneous demands on attention) to become significant. Informal rules described in the text would then become important and could lead to either HFE. The issue addressed in this analysis is to assess if *physical deviations* in the LLOCA initiator and base case scenario can adversely affect the operators in ways that have the potential to transform the DBA into a core damage. Because it appears that additional complications beyond the *physical deviations* in the LLOCA initiator are required for this case to have a reasonable likelihood of leading to the HFEs, the "No" LLOCA deviation case is dropped from further consideration in this analysis.[6]

[6]The interested reader will find that a very similar scenario was identified through a less direct process, in a trial of an earlier version of ATHEANA (NUREG-1624). That analysis proceeded by identifying potential HFEs; searching procedures and informal rules for rules that would direct the HFE, if used improperly; and then tried to add on plant and human context that would enable the HFE. There was no direct search for deviations or procedure mapping, so success depended on close familiarity with EOPs by operators on the analysis team and a rather free association of principles from behavioral science with plant conditions and the HFE, to complete the context. The scenario of the previous analysis included an initiating event that is nearly identical to the "No" LOCA deviation case; that analysis also identified significant failures in instruments. The conditional probability of the HFE and failure to recover was quite high (0.8 and 0.1). However, the plant-specific probability of the particular postulated instrument failure was very low, leading to a very small contribution to core damage frequency.

Table C.4 Application of Guide Words to LLOCA Deviation Analysis

Guide Word	Possible Physical Deviation	Significance	Carry Forward? (Explained in Text)
No/not/less/ late/never/too slow/too long / part of	Break size less than DBA	Can change timing, no longer have right conditions at EOP decision points. If the vulnerabilities identified in the text enable associated error mechanisms, operators could interrupt early makeup or fail to properly align sump recirculation cooling or RHR.	Yes
	Power fails to drop (fails to shutdown)	Only possible if pre-existing error violated fuel load/control requirements. Assumed very low probability.	Not evaluated further, at this time
	Reduced ECCS Flow	Reduced flow due to obstruction or impaired pump performance is either too great for success (and is therefore included in ECCS system analysis of the PRA) or impacts timing and RCS radioactivity, which does not appear to have significant impact on human performance.	No, little impact on operator performance
More/ Early/ Too Quick/ Too Short	Break size greater than DBA (i.e., greater than 2 loops or reactor vessel)	Not analyzed because very low in frequency and little impact on operator performance. Either the event is too severe for the ECCS to handle or not. The operator has no direct indication of LOCA size. However, because of redundancy in injection systems, and because full HPI adds significant flow, the plant could survive some such accidents. Can change timing, especially shortening the time to start and to complete switchover.	No, little impact on operator performance
Reversed	None	No physical sense other than inadvertent SI, which is another identified initiating event.	No, N/A
As well as/ repeated/ inadvertent	Switching; starts as near-DBA, plugging by debris, later return to LLOCA	Interim SLOCA leads to disabling LPI and automatic SI actuation, operators fall into a regime where they know what is going on Very low in frequency, but significant impact on operations.	Yes

Table C.5 Results of LLOCA Deviation Analysis

Possible Physical Deviation	Characteristics Potentially Affecting Human Response	Potential Error Types and Mechanisms	Further Analysis and Possible Similar Scenarios
"No" LLOCA Deviation Case: Break size less than DBA	Large change in parameter Low rate of change in parameter Relative rate of change in two or more parameters is not what would have been expected Changes in two or more parameters in a short time Direction of change in parameters over time is not what would be expected	A number of error types and mechanisms relevant to the HFEs (interrupt early makeup and fail to align recirculation) are associated with the characteristics Error types include lack of attention to other parameters, failure to take account of changes in parameter, failure to attend to more relevant parameters, or failure to recognize a serious situation in time can all lead to taking inappropriate action, taking correct action too soon, and failure to take needed action The underlying error mechanisms include over-eagerness, simplifying, preoccupation, tunnel vision, and fixation	The issue addressed in this analysis is to assess if *physical deviations* in the initiator can lead to core damage. This scenario is dropped from further consideration, because it almost surely requires additional context (e.g., instrumentation problems or significant extraneous demands on attention) to become significant.
"Switching" LLOCA Deviation Case: starts as near DBA, plugging by debris, later return to LLOCA	Large change in parameter Low rate of change in parameter, early on Relative rate of change in two or more parameters is not what would have been expected Changes in two or more parameters in a short time (following a period of stability) Garden path problem Situations that change Multiple lines of reasoning	A very large number of error types and mechanisms relevant to one HFE of Step 4 (fail to align recirculation) and a new HFE (fail to manually initiate LPI) are associated with the characteristics Error types include lack of awareness of change, generation of false theories to explain seeming anomalies, delay in response while searching for an explanation, lack of attention to other parameters, failure to take account of changes in parameter, failure to attend to more relevant parameters, or failure to recognize a serious situation in time can all lead to missing a decision point, taking inappropriate action, and failure to take needed action The underlying error mechanisms include incredulity, over-eagerness, simplifying, preoccupation, tunnel vision, fixation, lack of deep technical knowledge, and multiple lines of reasoning are creating conflicting choices	Yes, continue. Similar scenario: Small LOCA that stabilizes and later expands quickly to a near DBA LLOCA; similar scenario, but much more likely

Now consider the "Switching" LLOCA deviation case. This scenario has many nearly overwhelming error mechanisms at work. On top of that, although one can track a success path through the EOPs, there are many opportunities for missing, at least for a short time, necessary pieces of information. All this is combined with unfavorable timing (very short time frame for restarting RHR pumps; a distorted picture of the time until switchover to recirculation, and possibly, for switchover due to the long time under SLOCA conditions). Finally there is disbelief that a LLOCA can actually occur and the early confusion in the event. All together, this is a very strong EFC for the two HFEs under consideration.

C.6.2 Search of Relevant Rules

The EOPs applying to the base case LLOCA were examined in Section 5 and yielded no strong context that would be expected to lead to error without further EFC. In addition, the two more challenging deviation scenarios developed from applying the guide words to the base case LLOCA led to a thorough review of the EOPs applied to these scenarios, under the search of Section C.6.1. This search of the EOPs yielded several challenging conditions.

Because of the strong context already developed, no further search of the rules is needed here.

C.6.3 Search for Support System Dependencies

In some designs, there are large valves in the RCS loops that can be opened under RCS pressure. In addition, there could be some combination of pump seal ruptures that could equal a LLOCA. For such plants, human actions and the effects of support system failures (e.g., seal cooling systems) could induce a LLOCA. However, in this plant no support system induced failures and human actions have been identified that can mimic a LLOCA. There are no large valves that interface with the RCS that can be physically opened under normal RCS pressure. Likewise there are no combinations of pump seals, whose rupture is larger than an SLOCA.

A related issue is dependency among operator actions. It is possible that, if operators identify the need for restarting RHR pumps in time, there could be some dependency between that action and the eventual action to switchover to recirculation cooling. One was identified in the discussion of the "Switching" LLOCA scenario in Section C.6.1. Depending on which procedural anchor the operators use to start the RHR pumps, they can restart E-0, jump to E-1 Step 14, jump to ES-1.2 Step 3, or simply start the pumps and continue their cycle through ES-1.2. The likelihood of being ready for recirculation, when needed, may depend on this decision.

C.6.4 Search for Operator Tendencies and Error Types

This search could develop other potentially significant EFC that could become contributors to core damage frequency. However, it will not be performed, for two reasons:

- As indicated in the process description of Section 9.6.6, this search is a "catch-all" for deviation characteristics that might have been missed in the earlier searches. It is similar to

the open-ended search of earlier versions of ATHEANA, albeit a more structured approach. If significant EFC/UA combinations have been identified by the earlier searches, they are more likely to be important, because they focus on elements known to be represented in serious accidents

- It is outside the scope of the issue for which this ATHEANA analysis is performed. The issue is to determine if *physical characteristics* associated with the progression of the LLOCA can adversely affect the human operators in ways that have the potential to transform the DBA into a core damage accident.

C.6.5 Develop Descriptions of Deviation Scenarios

The description of the "Switching" LLOCA in Section C.6.1 is complete and has not been extended by searches in C.6.2, C.6.3, or C.6.5, because the context was deemed strong enough without further requirements that diminish the frequency of the event. Likewise, while additional complicating factors would make the context even more cognitively demanding, the scenario and possible unsafe acts, as already postulated, seem sufficiently challenging. Therefore, additional complicating factors will not be added at this time.

It is appropriate, at this point to summarize the key elements of the "Switching" LLOCA scenario; identify those vulnerabilities, error types and potential error mechanisms that we believe are most significant; and identify the associated PSFs. This information is presented in Table C.6.

C.7 Step 7: Identify and Evaluate Complicating Factors and Links to PSFs

This step is addressed in section C.6.5 above.

C.8 Step 8: Evaluate the Potential for Recovery

Because of the short time available for restarting RHR pump, the short time later when switchover to recirculation must begin, and the short time available to complete the switchover, recovery is not considered separately. Definition of the HFEs will include the idea that failure means failure to accomplish the activity, within the time before unrecoverable damage occurs.

C.9 Step 9: Quantification Considerations

Quantification of the "Switching" LLOCA deviation case will focus first on the probability of the unsafe acts (UAs), given the scenario. The reasons for this are explained in more detail in the following section on issue resolution.

Probability of Unsafe Acts. We address the probability of the UAs including non-recovery in an integrated one-step process. Thus we evaluate

Table C.6 "Switching" LLOCA Deviation Scenario

Overall Plant Condition (Scenario)	Key Information Related to HFEs, Error Types, and Error Mechanisms	Most Relevant PSFs
Event starts as near DBA LLOCA. After the initial few second of response, plugging by debris occurs and the event continues as an SLOCA. Later, after the operators have stabilized the SLOCA and are preparing for long term cooling, the debris vibrates free and the LLOCA returns.	Two HFEs of interest (fail to align recirculation) and (fail to manually initiate LPI) Unexpected initial events can lead to false theories to explain seeming anomalies caused by incredulity; this allows the initial information to create early confusion and to become lost later, when it would be helpful As operators settle into the SLOCA track, they become vulnerable to the garden path problem and are susceptible to tunnel vision and fixation, simplifying the scenario by ignoring the initial LLOCA-like trends When RHR pumps are secured, the procedure warns that manual restart would be required. Nevertheless, experience and training reinforce the garden path scenario As they begin to focus on moving out of SI and into RHR cooling, they can become preoccupied with the details of EOP ES-1.2 and developing an over-eagerness to reach the stable end point All these factors permit a lack of awareness of change and of attention to other parameters Now they are set up for failure to recognize a serious situation in time; i.e., they can miss a key decision point, failing to take needed action, when RCS pressure suddenly falls because of the reinitiated LLOCA Even if they should respond in time, restarting the RHR pumps, multiple lines of reasoning about where to branch in the EOPs creates conflicting choices, delaying their attention from preparing for recirculation cooling, which will be needed very soon	Training/practice. Lack of training or practice for off-normal, unexpected accident conditions and problem solving Training/practice. Base case LLOCA and SLOCA used repeatedly in training Procedures. Insufficient warning to be prepared for rapidly increasing LOCA Lack of trending displays allows odd initial parameter tracks to be put aside

$P(UA_1)$ = P(operators fail to restart RHR pumps | EFC), and

$P(UA_2)$ = P(they fail to complete the sump recirculation cooling lineup before the RWST runs dry | they restart RHR pumps $\wedge$ EFC)

Taking into account the deviation scenario, including the associated EFC documented in Table C.6 and the short time available for each action, the analysts have developed a consensus judgment of the likelihood of the crew performing these unsafe acts. Their judgment is based on their experience, their observations of many crews in the plant and in simulators, and their understanding of the context of this event, including the status of procedures and training discussed earlier. Given the difficult context of the scenario our estimates are

$P(UA_1)$ = 0.30; i.e., they are only slightly more likely to restart the pumps than not

$P(UA_2)$ = 0.07; i.e., about 1 in 15 crews would be trapped by the short time, multiple lines of reasoning, and deceptive timing and fail to shift to recirculation in time[7]

Frequency of Error-Forcing Context. To be consistent with the PRA, we estimate the frequency of LLOCA as 1×10^{-4} per year. The conditional probability of the "Switching" LLOCA, given a LLOCA would generally be quite low, we believe, although there is no direct experience with LLOCAs in PWRs to demonstrate that real LLOCA forces in an aged, real plant would not result in unexpected structural failures. For our particular plant, a recent SG internal inspection identified indications in the steel sheet that separates the T_H and T_C plena that were believed to be insignificant, but were scheduled for a detailed examination at the next refueling outage. Under this condition

[7]As a sanity check on these estimates, we examine the suggested values for generic tasks of a similar nature from the HEART methodology summarized in Section 10. First we must match our actions and EFC with those in HEART. The following are reasonable matches:

- Restarting the RHR pumps, is, in the words of HEART a "routine, highly practiced, rapid task involving relatively low levels of skill, but EFC is "unfamiliarity with a situation that is potentially important, but which occurs infrequently or is novel." The associated probability is no more than 17 * 0.02 or 0.34, with uncertainty of (0.12 to no more than 0.77)

- Switchover to recirculation cooling, is, in the words of HEART almost a "complex task requiring a high level of comprehension or skill." It is tempered by the fact that they did restart the pumps and hardened by the strength of the EFC. If we assume that the positive impact of having restarted the pumps balances the difficult EFC, the associated probability from HEART is 0.16 and ranges from 0.12 to 0.28.

Our estimate for UA_1 is surprisingly consistent with the generic estimates in HEART. Our estimate for UA_2 is lower than HEART by about a factor of 2; i.e., reasonably close.

combined with the forces of the LLOCA, the conditional probability of cracking and displacement of that sheet and later shifting as pumps are started and stopped is judged to be 1 in 10. So the frequency of the "Switching" LLOCA is 1×10^{-5} per year, for this particular plant.

Frequency of the Event Leading to Core Damage. Combining the frequency of the EFC and the probability of the HFEs yields an estimate of core damage frequency due to the physical deviation of the "Switching" LLOCA scenario creating an EFC that sets up the operators for failure. To have failure, either the operators fail to restart RHR pumps or they successfully start the pumps and fail to complete the sump recirculation cooling lineup before the RWST runs dry; i.e.,

$$P(UA_1) + \{[1 - P(UA_1)] * P(UA_2)\} = 0.35$$

Combining the frequency of the EFC with the probability that one of the UAs occur yields a core damage frequency of 3.5×10^{-6} per year for the "Switching" LLOCA deviation case.

C.10 Issue Resolution

This ATHEANA example analysis was performed to address one specific issue:

> *To determine if physical characteristics associated with the progression of the LLOCA initiator can adversely affect the human operators in ways that have the potential to transform the DBA into a core damage accident.*

The analysis defined several deviation scenarios in Table C.4 that go beyond training and FSAR analysis and could lead to core damage. Two of them are functionally challenging, but would not seem to challenge the operators. One, "Power fails to drop," could be very challenging to the operators, but it would appear to be very unlikely, and was dropped from the analysis without substantial investigation into its plausibility. Of the remaining two, the "No" LLOCA deviation case (< DBA) was shown to involve many possible human error mechanisms, but was believed to require additional complications for the HFEs to have a substantial chance of occurring. It goes, therefore, beyond the issue defined for the analysis and was dropped, but flagged as a case worthy of investigation under other issues.

The remaining case, the "Switching" LLOCA involves many challenging aspects. The probability of an HFE, given the scenario, is quite high. In a generic sense, the frequency of this initiator is very, very low. Nevertheless, there are several reasons to consider the case seriously:

- It is more than frequency. In the spirit of medical diagnosis, it is not simply the probability of a possible diagnosis that is of interest. If some very high consequence *treatable* disease has a low probability of being correct, we hope our physician does not dismiss it, because of its low probability, but investigates further (more research on the characteristics of the

disease, more tests, etc.). We are more willing to play the odds, if the consequences are low. This is not to say that risk is not a suitable criteria for programmatic decision making, but that in diagnostics, it is worthwhile digging deeper and being better prepared for high consequence events.

- The frequency might not be correct. There may be failure modes not yet evidenced that can occur under specific conditions, including aging. Even if generically the chance of the "Switching" LLOCA may be very low, specific plants with specific designs, operating histories, maintenance histories, and vulnerabilities could have a much higher frequency for such events.

- Similar events. As identified in Table C.5, an SLOCA that stabilizes and later expands could have similar consequences, but higher frequency. Other possibilities include a smaller, more likely LLOCA combined with:

  - one RHR pump out of service and a second that was allowed to run "too long" in the operators' view such that they believe it is damaged.

  - Channel B Pzr pressure instrument out of service and the operators disbelieve Ch. A

Thus the issue resolution process may demand that the analysis be extended or that, because of the broad range of possibilities, some precautions in training or practice be instituted to ensure, if an unlikely or unforseen condition arises, the operators are well prepared to deal with it.

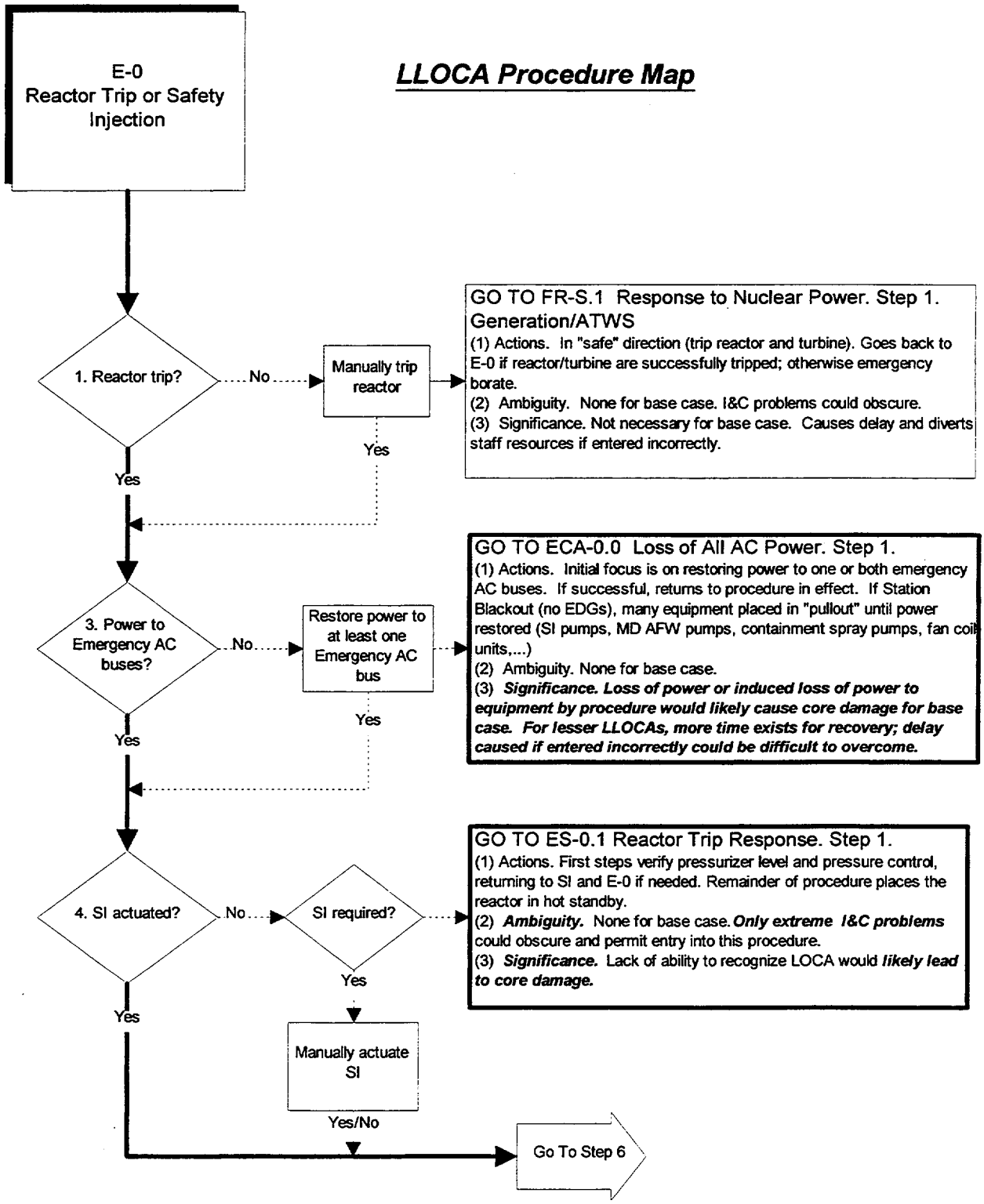


Figure C.13 EOP Map for Base Case LLOCA (Sheet 1)

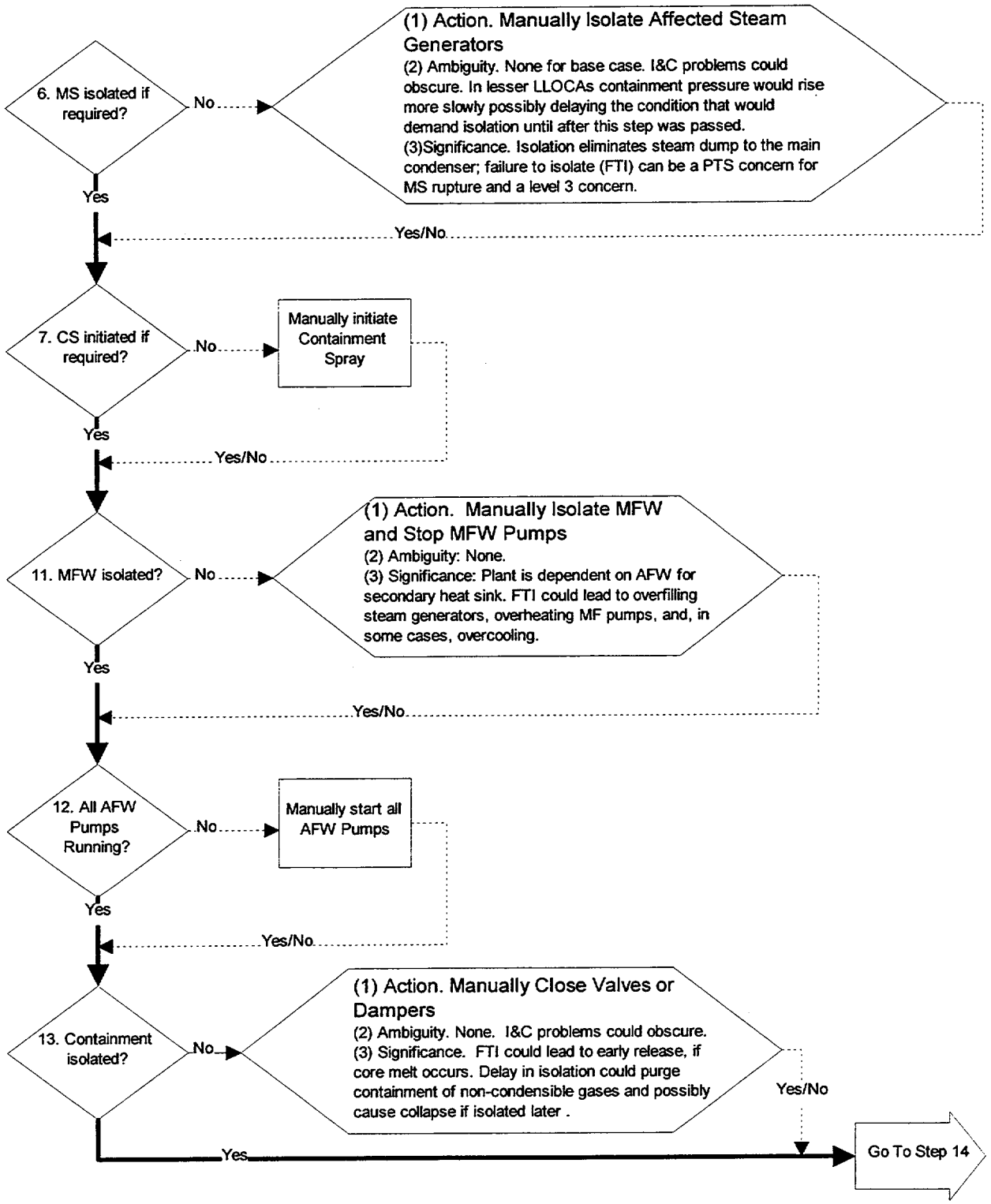


Figure C.13 EOP Map for Base Case LLOCA (Sheet 2)

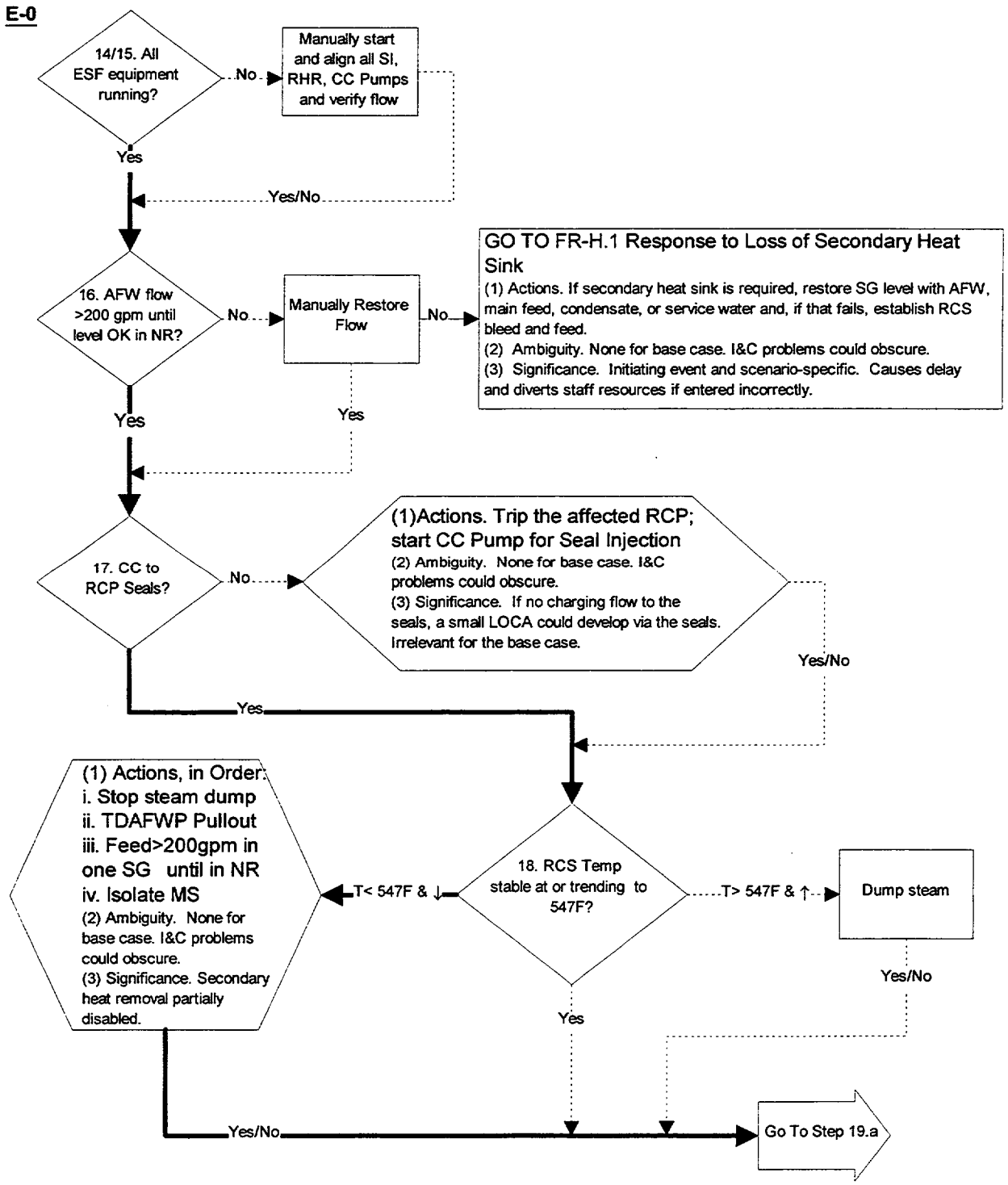


Figure C.13 EOP Map for Base Case LLOCA (Sheet 3)

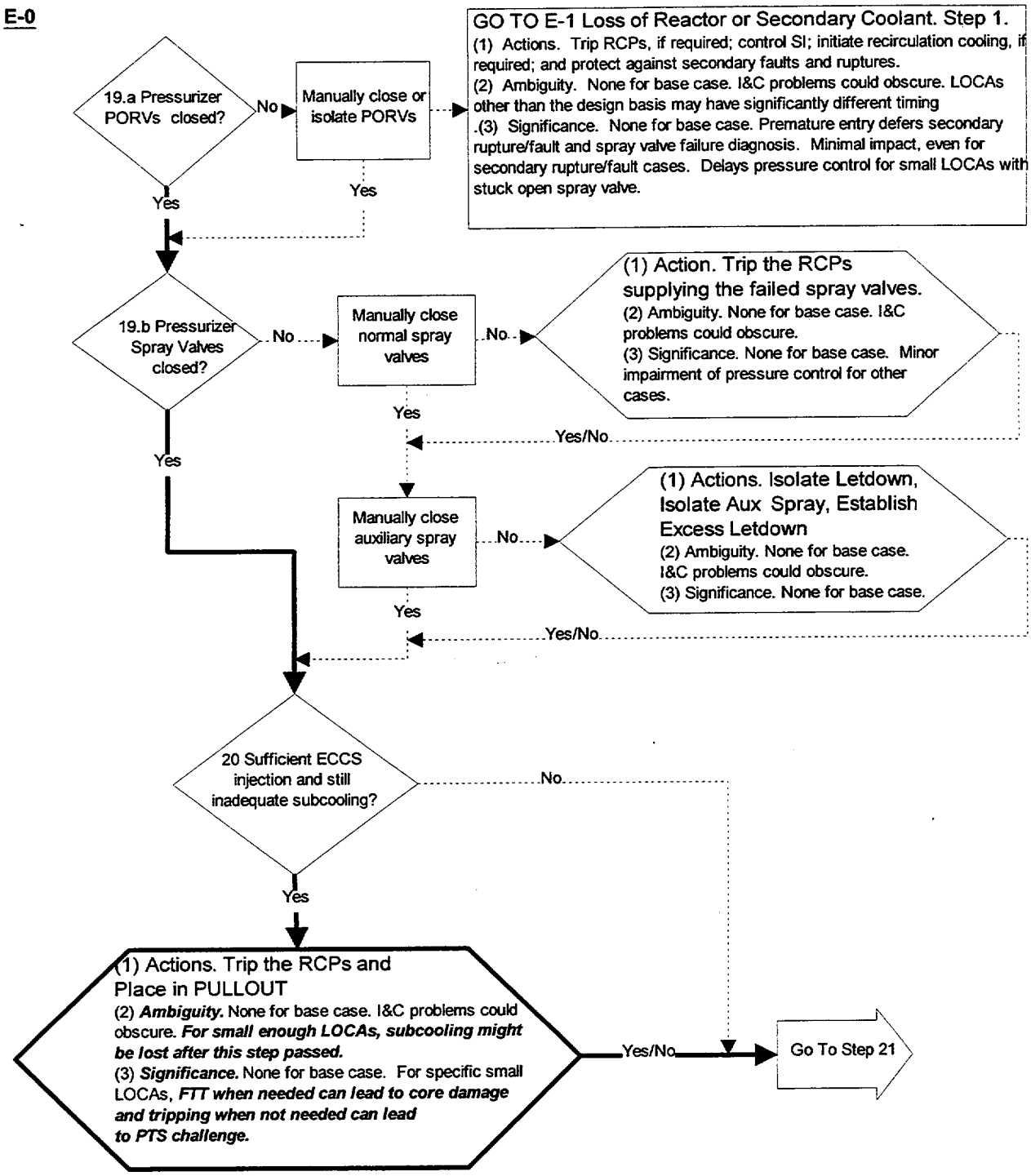


Figure C.13 EOP Map for Base Case LLOCA (Sheet 4)

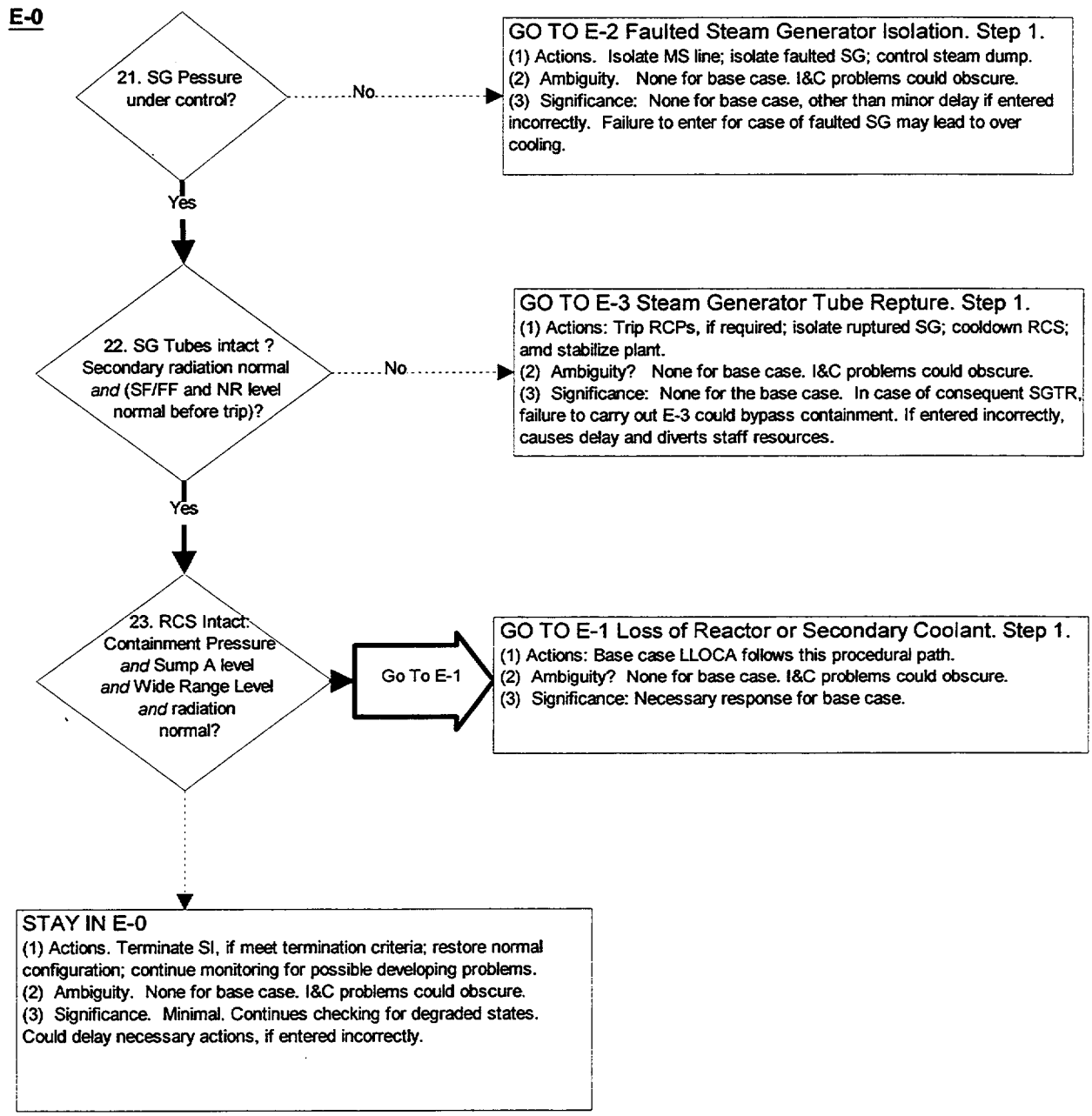


Figure C.13 EOP Map for Base Case LLOCA (Sheet 5)

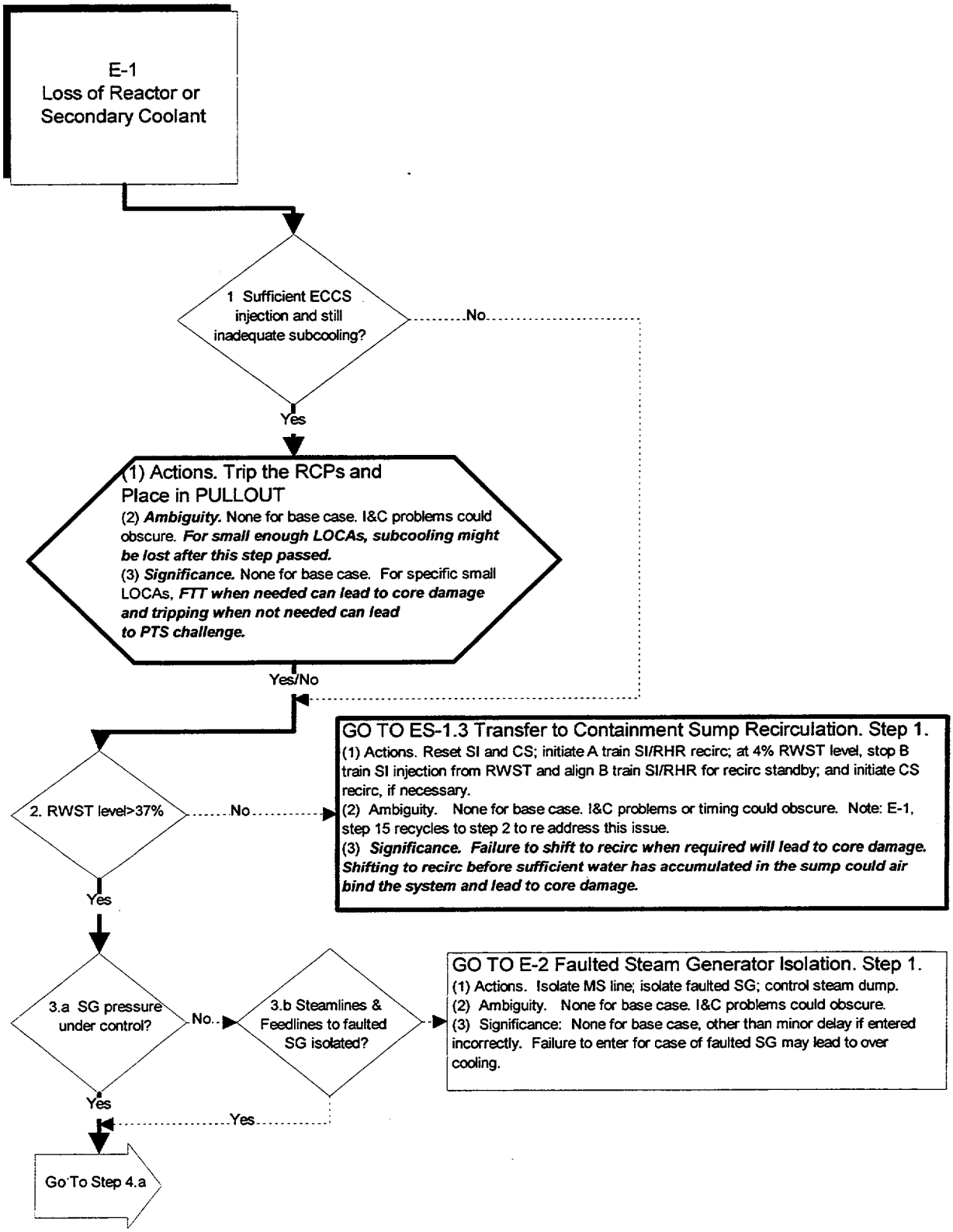


Figure C.13 EOP Map for Base Case LLOCA (Sheet 6)

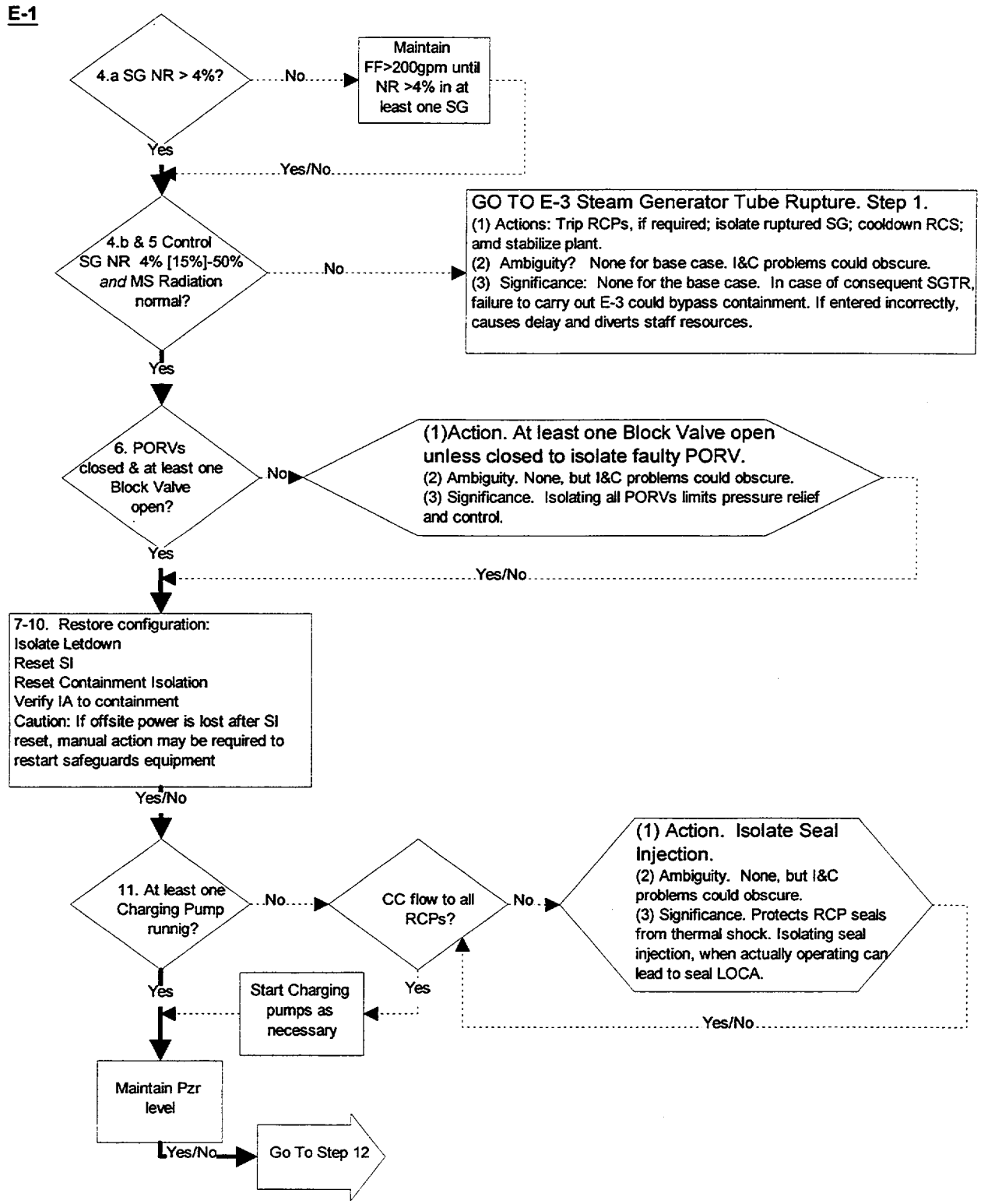


Figure C.13 EOP Map for Base Case LLOCA (Sheet 7)

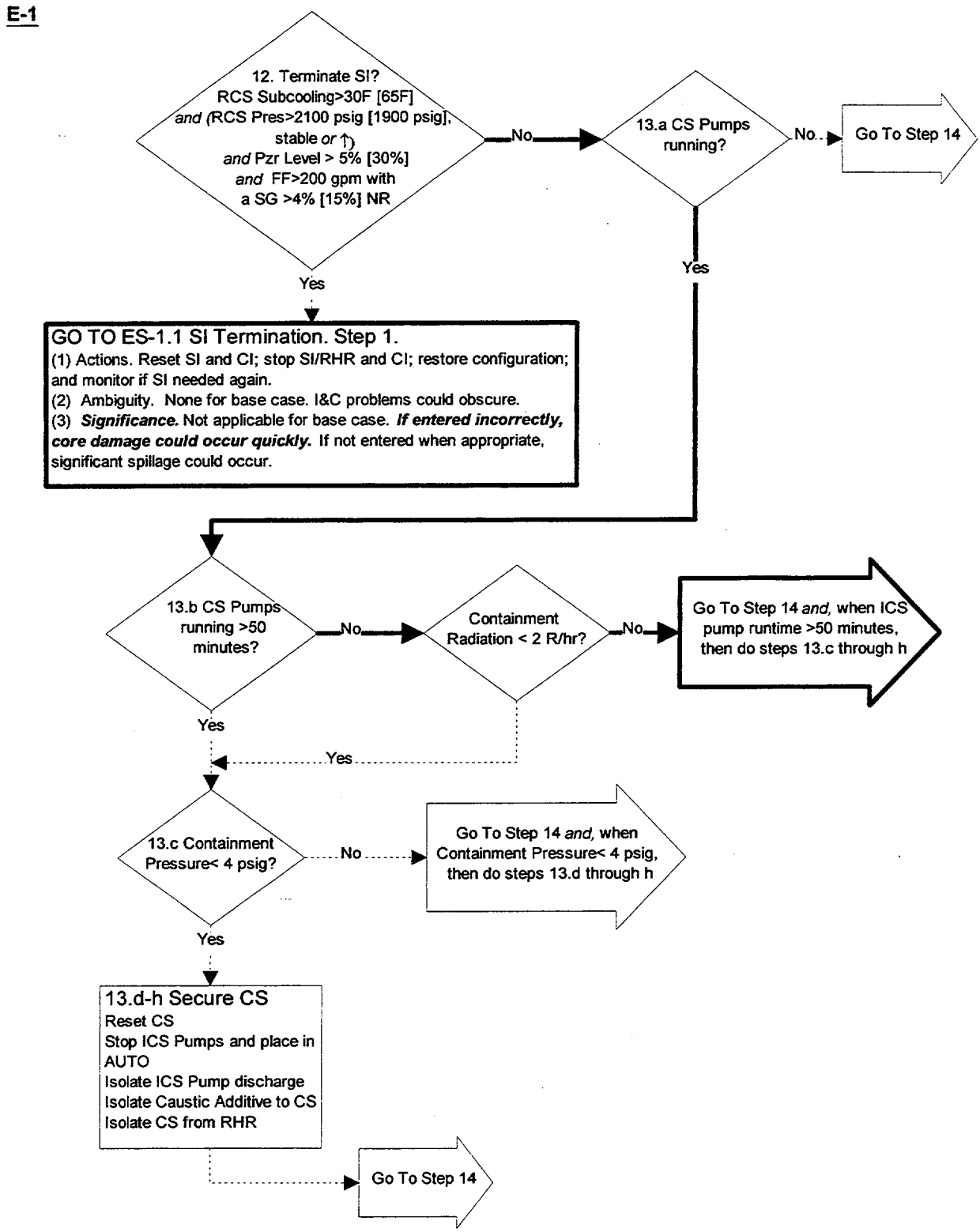


Figure C.13 EOP Map for Base Case LLOCA (Sheet 8)

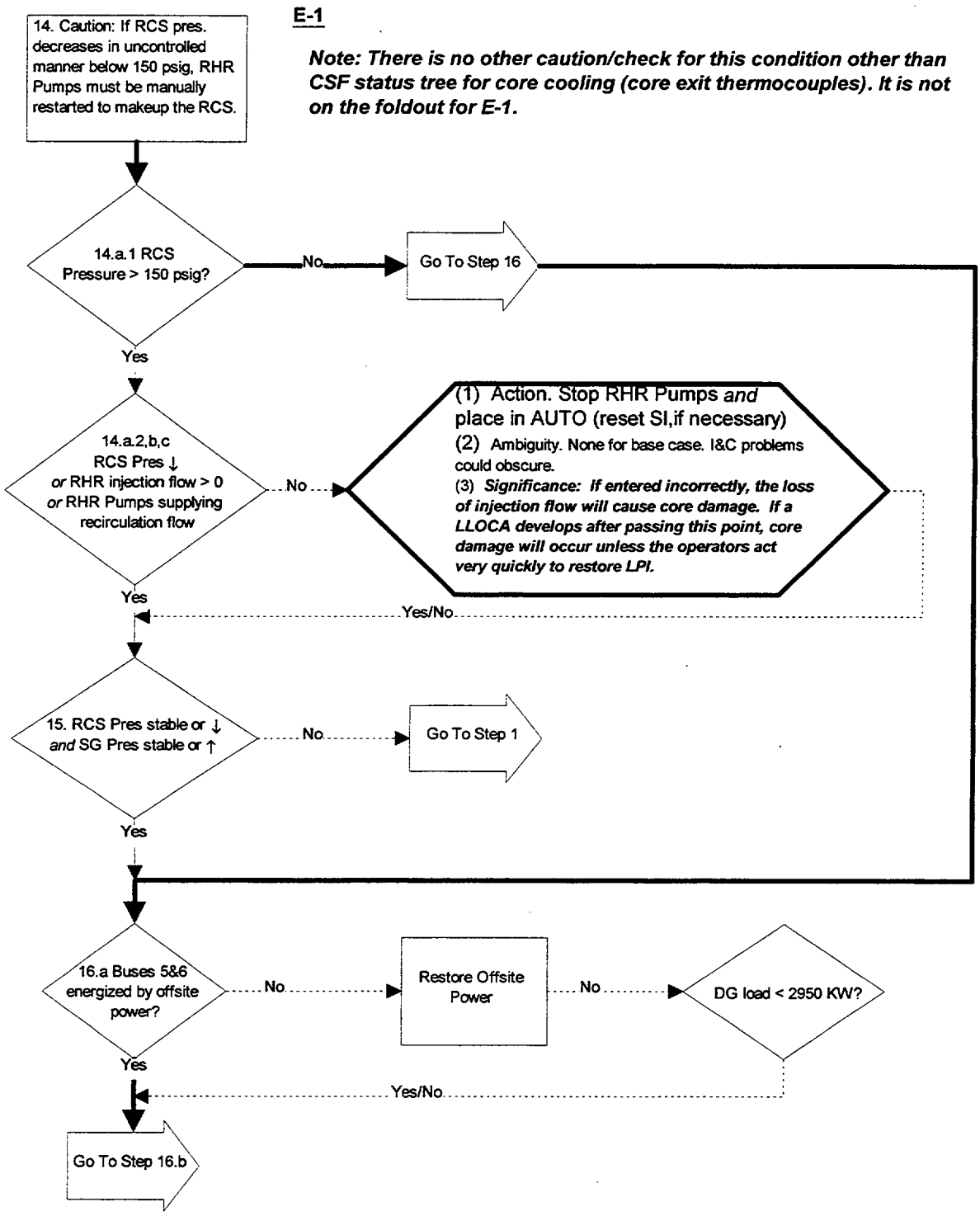


Figure C.13 EOP Map for Base Case LLOCA (Sheet 9)

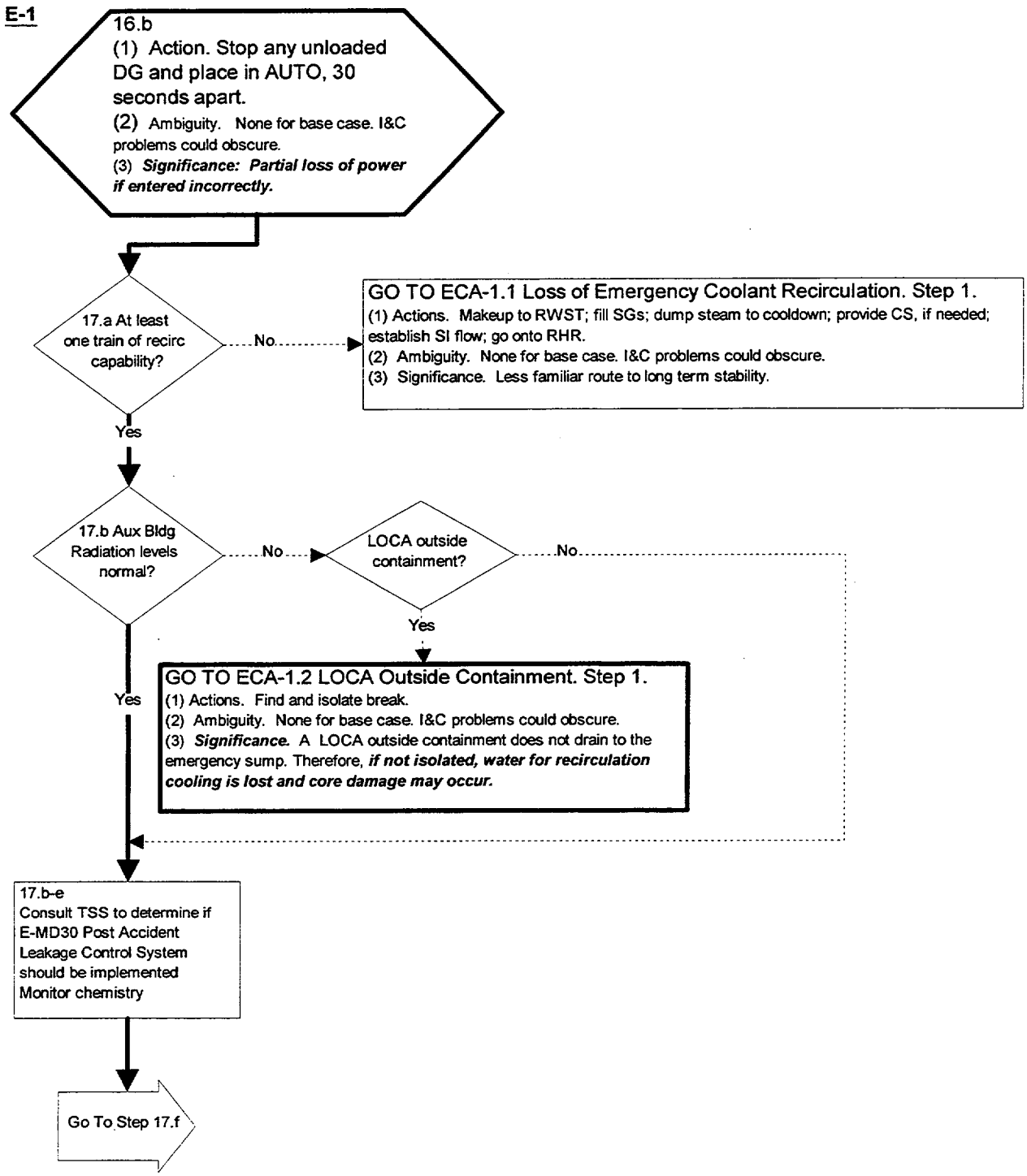


Figure C.13 EOP Map for Base Case LLOCA (Sheet 10)

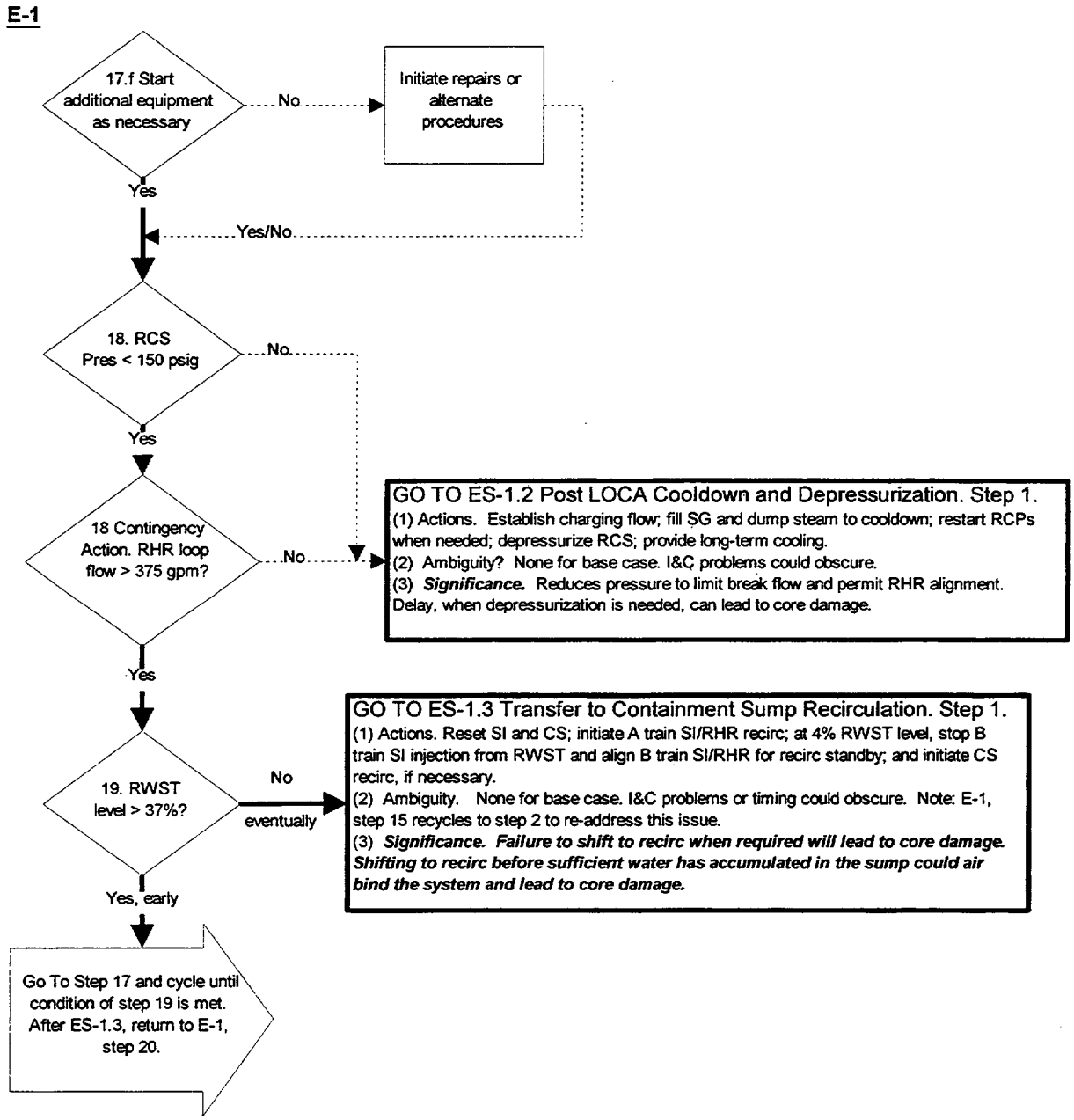


Figure C.13 EOP Map for Base Case LLOCA (Sheet 11)

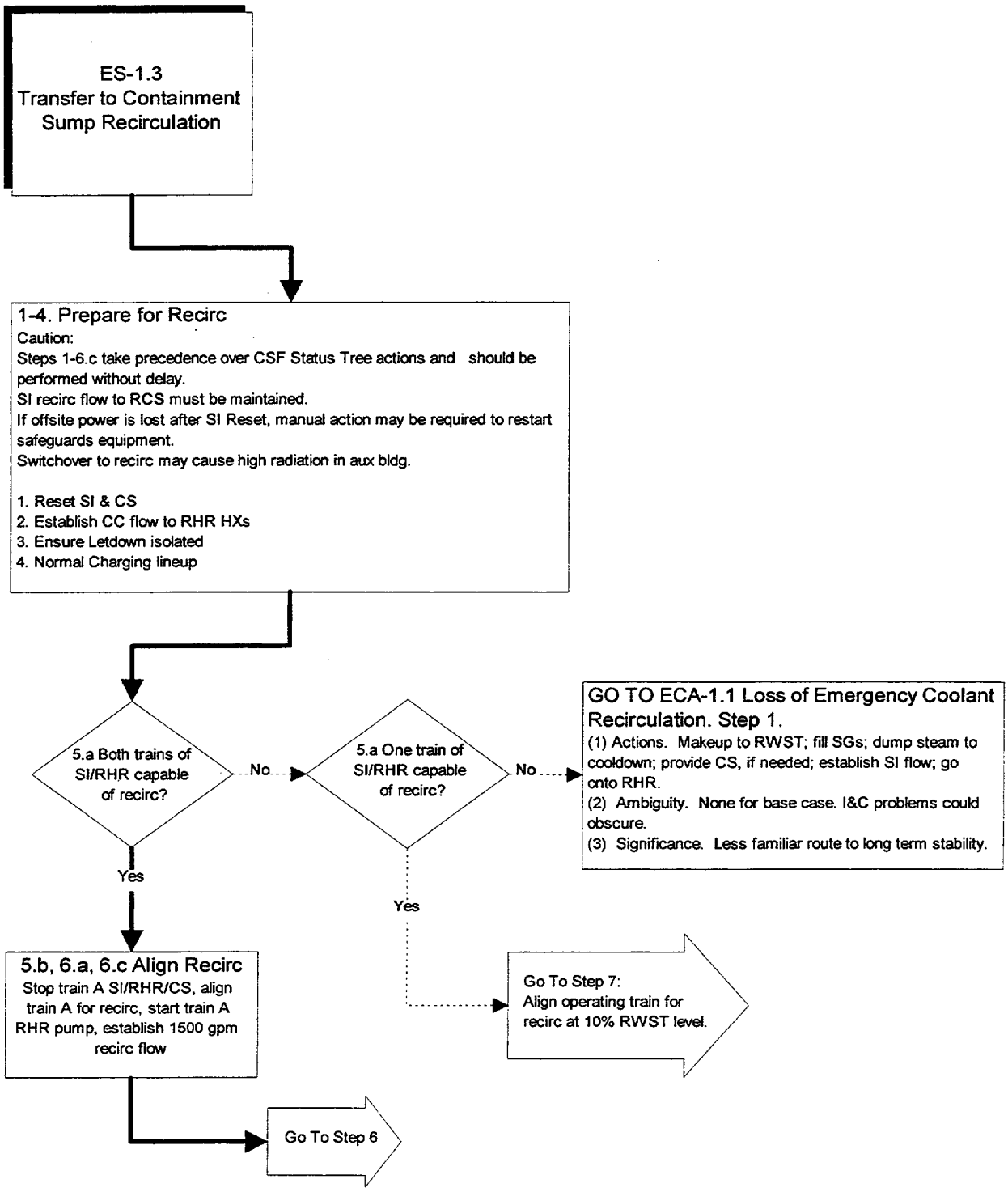


Figure C.13 EOP Map for Base Case LLOCA (Sheet 12)

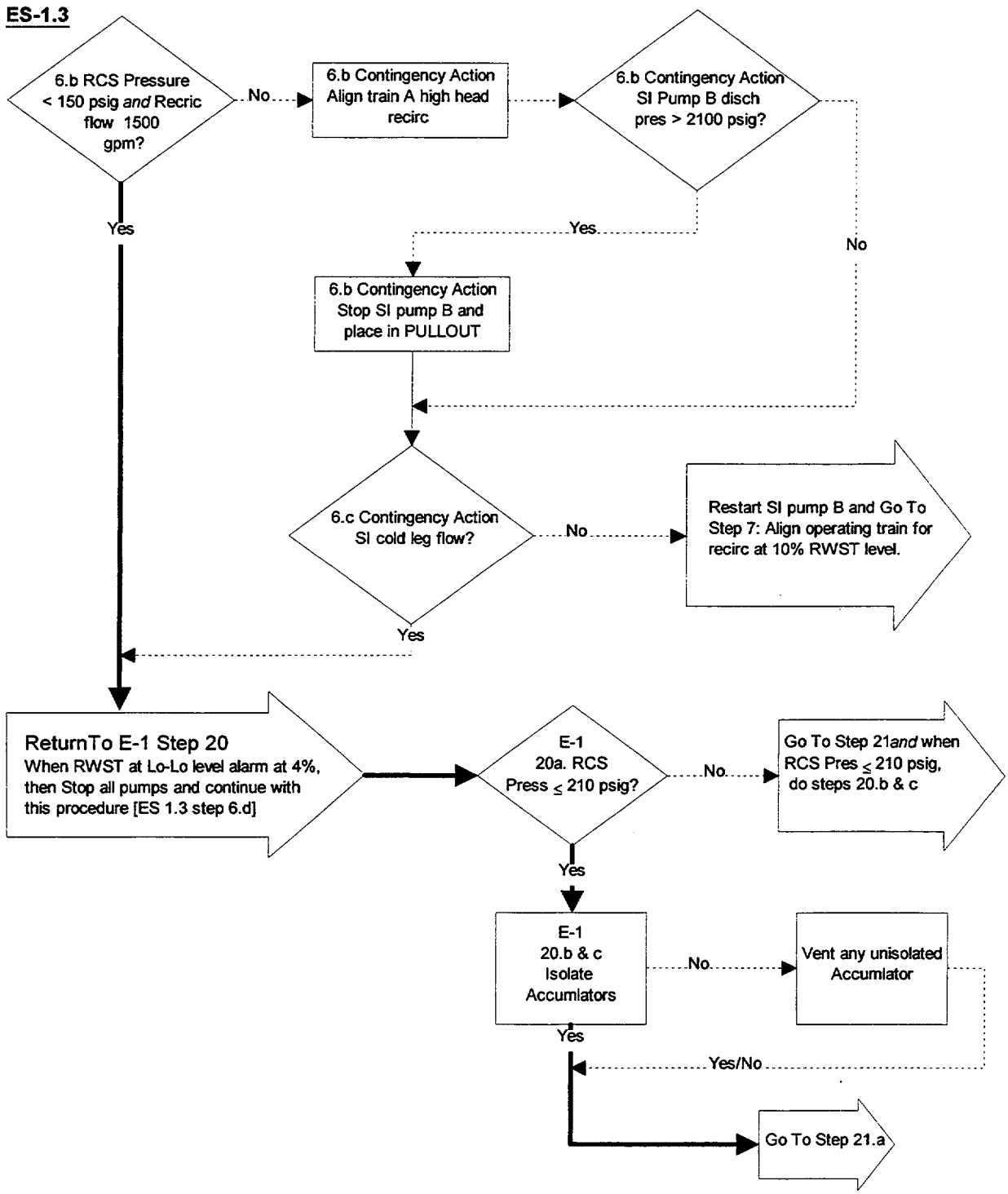


Figure C.13 EOP Map for Base Case LLOCA (Sheet 13)

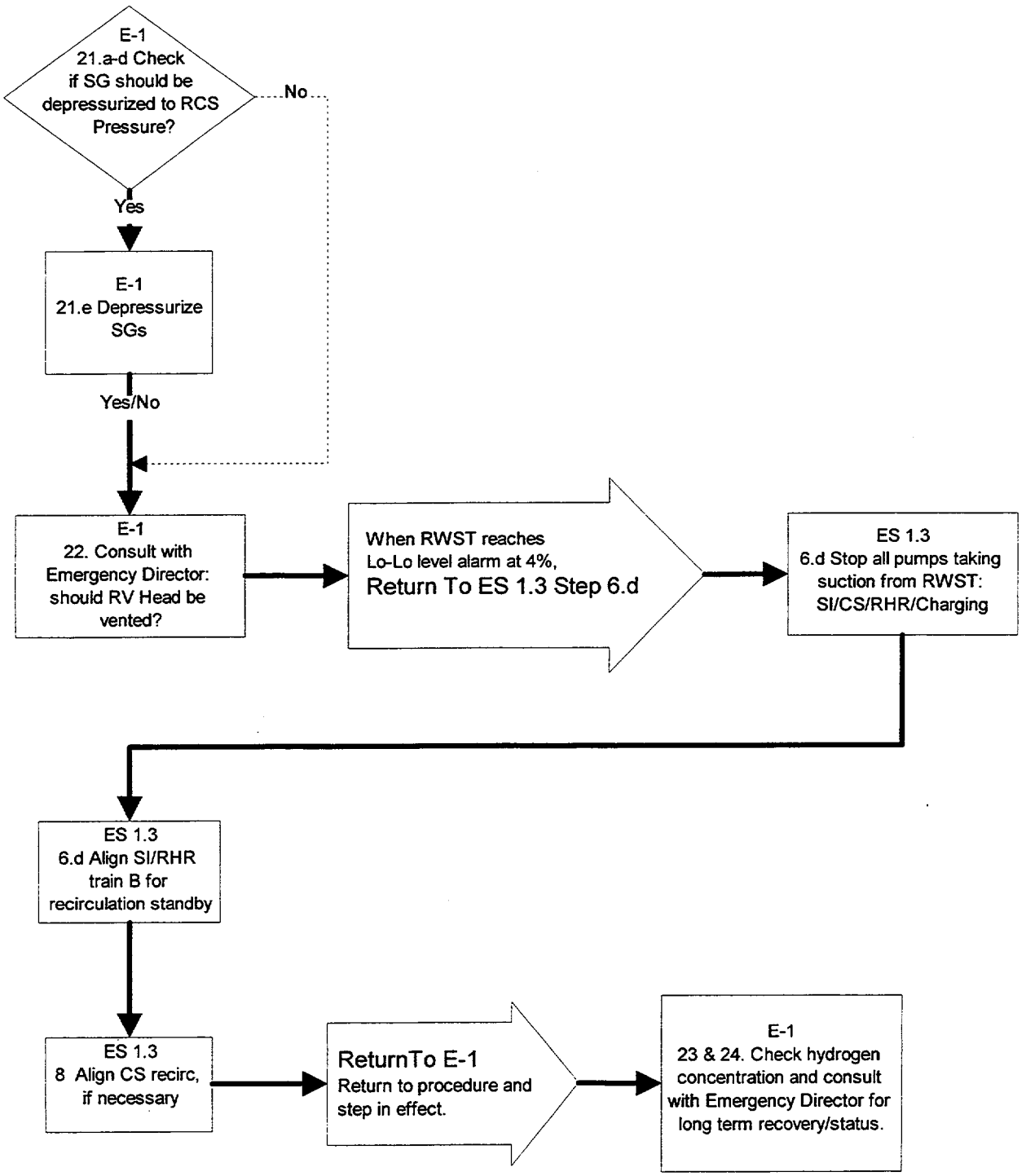


Figure C.13 EOP Map for Base Case LLOCA (Sheet 14)

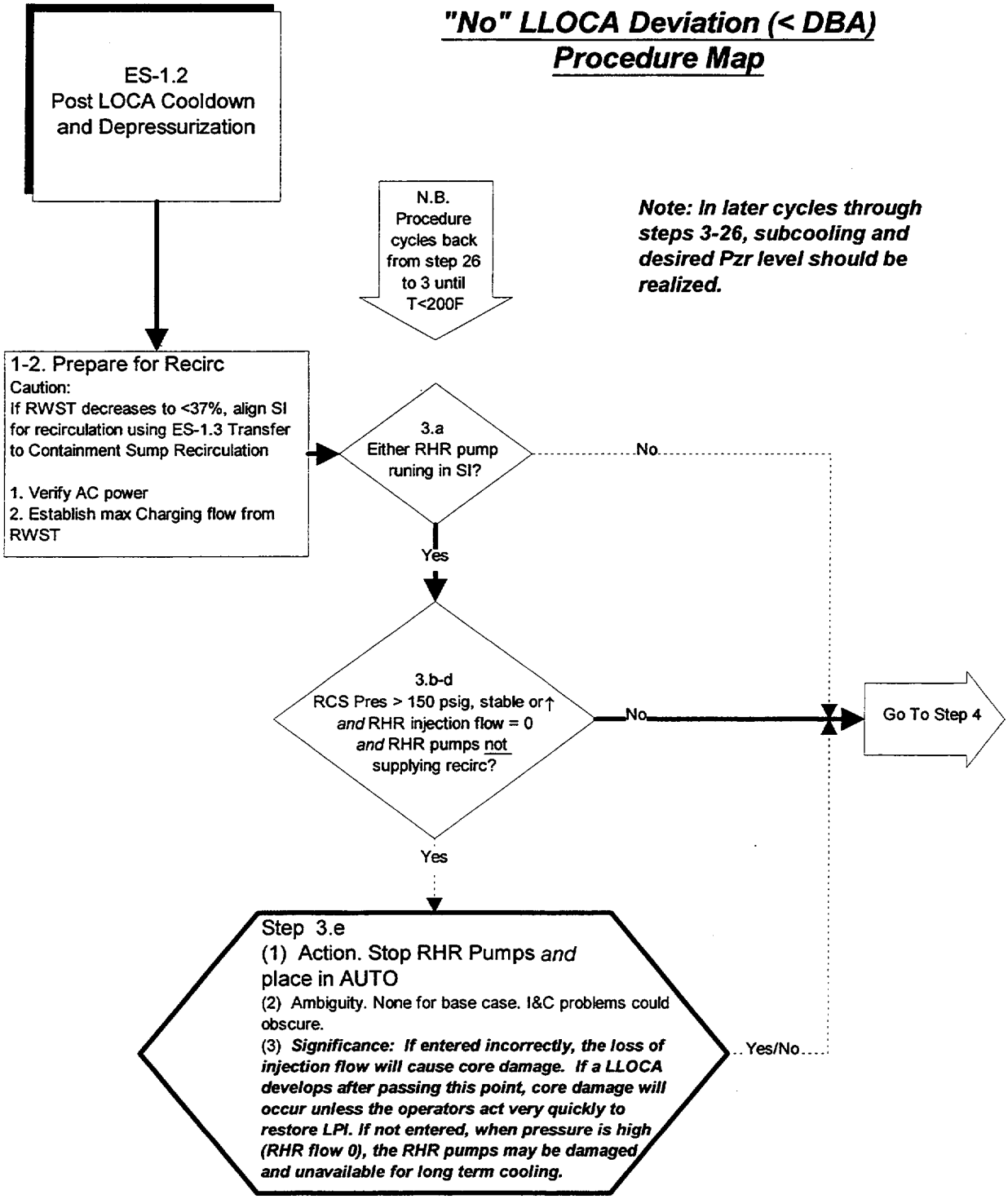


Figure C.15 "No" LLOCA Deviation (<DBA) Procedure Map (Sheet 1)

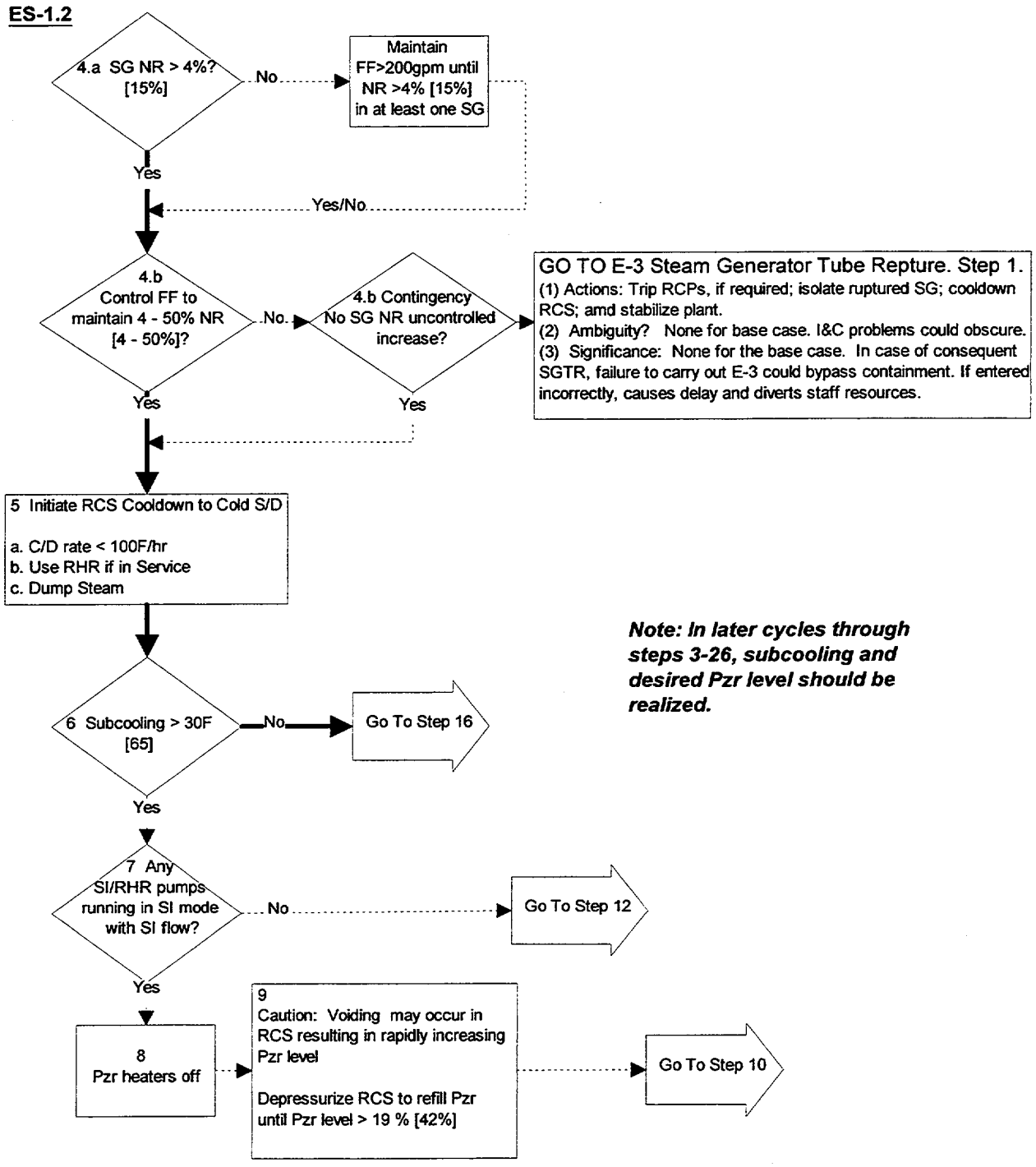


Figure C.15 "No" LLOCA Deviation (<DBA) Procedure Map (Sheet 2)

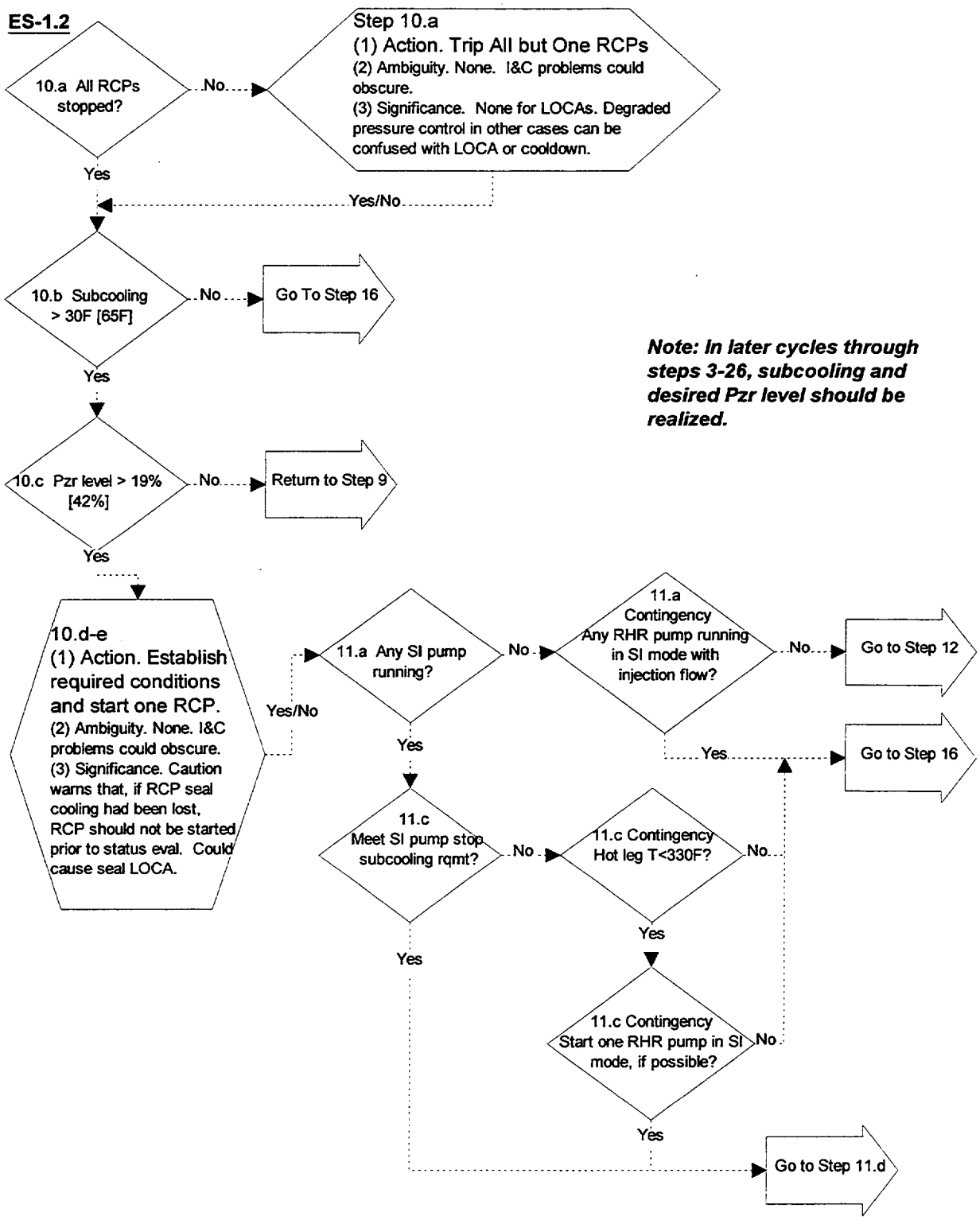


Figure C.15 "No" LLOCA Deviation (<DBA) Procedure Map (Sheet 3)

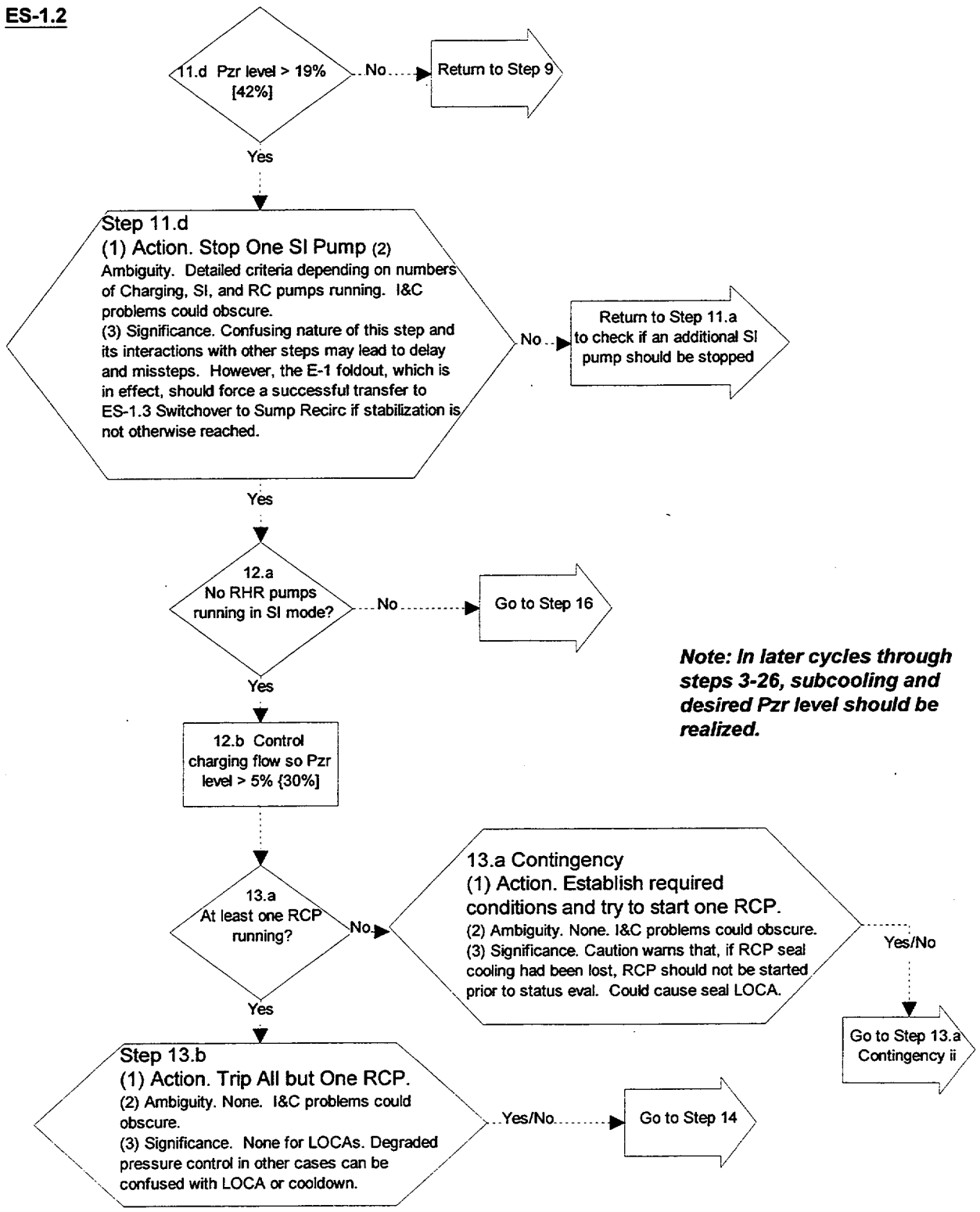


Figure C.15 "No" LLOCA Deviation (<DBA) Procedure Map (Sheet 4)

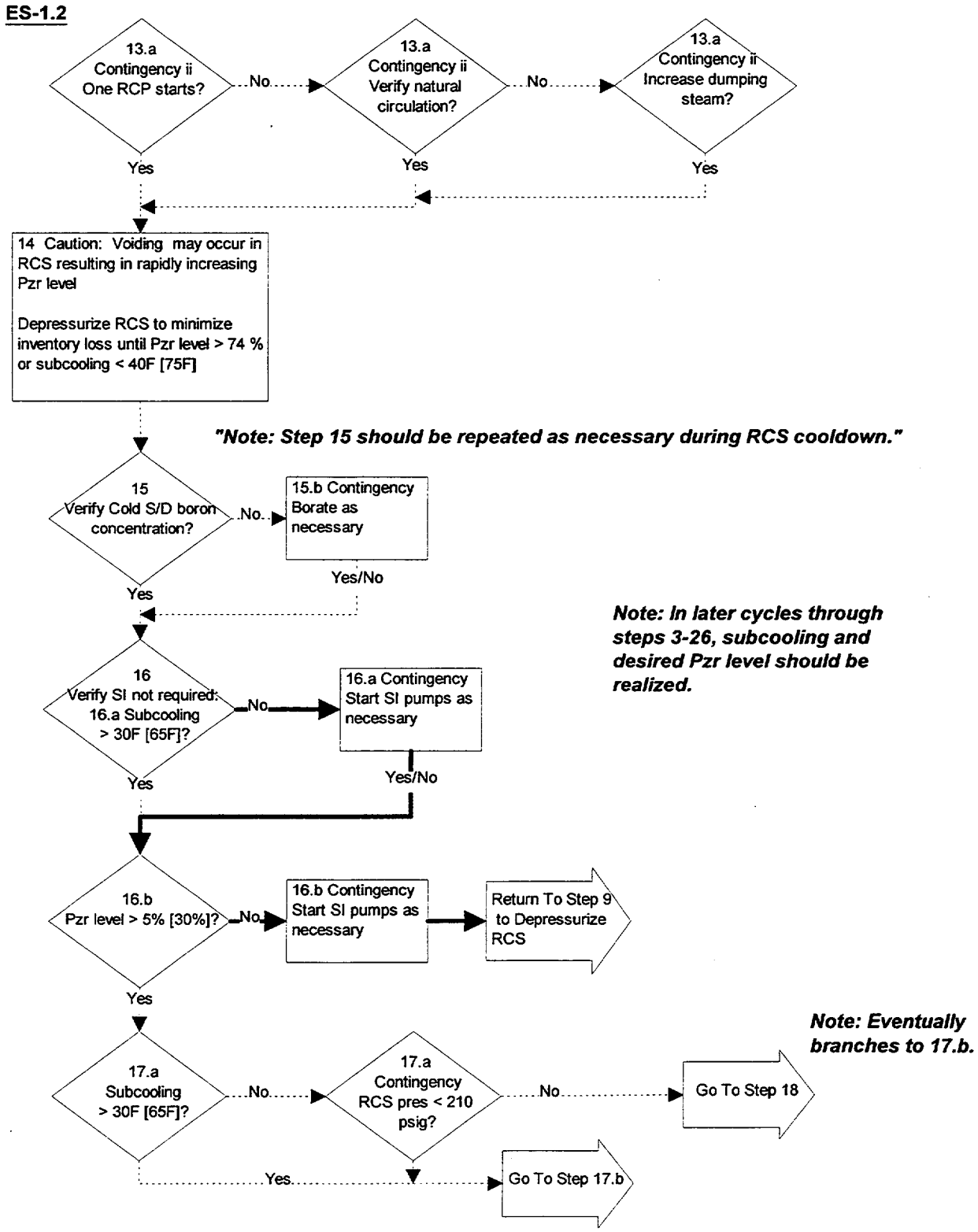
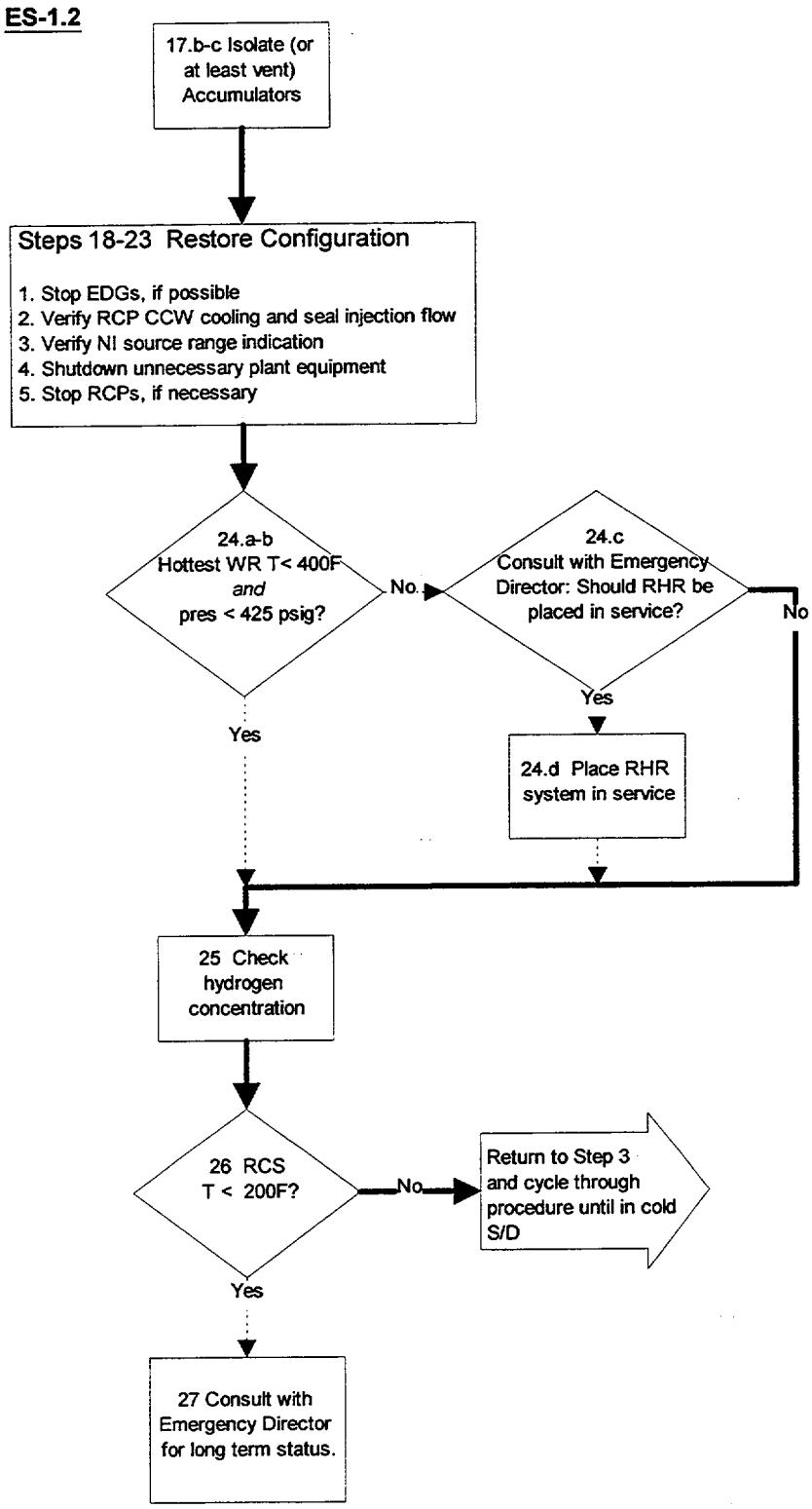


Figure C.15 "No" LLOCA Deviation (<DBA) Procedure Map (Sheet 5)



N.B. If RWST level cannot be maintained, the system must eventually be placed on RHR or the E-1 foldout will require going to ES-1.3 Transfer to Containment Sump Recirculation, Step 1

Figure C.15 "No" LLOCA Deviation (<DBA) Procedure Map (Sheet 6)

APPENDIX D
ATHEANA EXAMPLE -
LOSS OF SERVICE WATER EVENT

This appendix illustrates the use of the ATHEANA process to investigate the potential for operator actions that would degrade the plant response in a boiling water reactor (BWR) during a total loss of service water. In particular, the objective is to identify whether there are any improvements that would better prepare operating crews to properly respond to a prolonged loss of heat sink. Service water provides the ultimate heat sink in this BWR-6 design and without it, plant equipment will fail over time and the plant status will continue to degrade, potentially leading to core damage if the heat sink is not eventually restored. Thus actions that operators can take to "buy time" and maintain safety functions until the heat sink is restored are vital to the success of mitigating such an event. This illustration of the use of ATHEANA serves to identify those circumstances (contexts) that might induce human actions that would inappropriately worsen the plant response to the event, even though the operating crew is attempting to perform the appropriate responses. Put another way, the purpose of this analysis is to identify the more likely circumstances and the resulting errors that might be performed that would worsen the plant response in a loss of service water event.

While this is a plant-specific example, however, the plant analyzed is a composite BWR, not exactly matching any particular installation. The example is realistic in that all specific design, procedures, training and operating and maintenance practice information used in the analysis have been observed in real plants. As a result, this example provides a basis for licensees desiring to investigate a similar issue at their plant. The example follows the steps discussed in the ATHEANA process in Section 9 of this document.

D.1 Step 1: Define and Interpret the Issue

In this example, the issue being analyzed is the following:

> A prolonged loss of service water event at a BWR, while relatively unlikely compared with many other types of transients, represents a severe challenge to the plant. It is also an event that provides a significant challenge to the operating crew since they need to continually take actions to deal with the progressively deteriorating nature of this accident. If service water is not eventually restored, damage to plant equipment and potentially the core are possible. This event most likely involves multiple active failures or unlikely passive failures and is therefore beyond the design basis of the plant. Thus, procedures and training are limited, as are investigations into the complexities of operator response.
>
> The objective of the analysis is to identify whether there are any improvements that would better prepare operating crews to properly respond to a prolonged loss of ultimate heat sink. To do this, the analysis will identify (a) the possible conditions that might induce the operating crew to inappropriately respond to a prolonged loss of service water event and (b) the more likely errors by the operating crew that might occur as a result of these conditions. The results of the analysis are to be used to make any improvements (procedure changes, training changes, human–machine interface changes) that would better prepare the operating crews to properly respond to such a severe event.

D.2 Step 2: Define the Scope of the Analysis

The scope of this analysis has been largely based on the description of the issue provided in Step 1 where the initiating event is defined as a prolonged loss of service water. In addition, the scope is purposely limited to a scenario that does not include additional, random failures since the event itself already provides for progressive degradation of equipment in the plant over time. In fact, a review of Table 9.2 in Section 9 shows that this event by itself has the characteristics of a high-priority initiator. With the exception of "short time to damage" and "high frequency event," the loss of service water contains all the other characteristics presented in that table, even without other equipment failures.

The plant's probabilistic risk assessment (PRA) already covers the loss of service water initiating event and estimates a resulting core damage frequency of approximately 2E-7/year. This assessment is largely based on equipment failures and does not address potential operator actions other than some key errors of omission, such as failing to use firewater as an injection source (to buy time) and failing to restore service water. The PRA does not address possible errors of commission that might occur and make things worse, as a result of responding to the conditions in the plant as they develop. This ATHEANA analysis examines the potential contexts and the likelihood of the operating crew carrying out unsafe acts due to those contexts during their response to the event. Acts of concern include those that would make conditions worse, thereby lessening the time available to restore the ultimate heat sink.

D.3 Step 3: Describe the Base Case Scenario

D.3.1 Introduction

This step of the analysis process defines a base case scenario for the loss of service water event from which to develop scenario contexts that may challenge the operating crew in ways that may be error forcing. As stated earlier, this analysis will not pursue additional random failures during the scenario, but will examine likely deviations as a direct result of the event itself. Ideally, the base case scenario has the characteristics shown in the first row of Table D.1; i.e., the scenario description represents a consensus of the expected plant response by most operators, it is well defined operationally, there are well-defined physics descriptions and adequate documentation of the plant response, and the scenario is realistic. The base case scenario for this analysis has the characteristics shown in the second row of Table D.1.

As indicated in Table D.1, there is no consensus operator model or safety analysis report-based (SAR) reference case for this event. Nevertheless, information summarized in the next subsection provides the essentials for understanding the loss of service water event based on the plant design, existing procedural guidance and related operator expectations, and the PRA. From this information, a realistic base case scenario is derived using additional judgment on the part of the analysis team.

Table D.1 Base Case Scenario Characteristics

Base Case	Consensus Operator Model	Well Defined Operationally	Well-Defined Physics	Well Documented	Realistic
Ideal	Exists	Yes	Yes	Yes	Yes
Loss of service water scenario	No single model exists although some general expectations do exist for the short term.	No, since the specific effects on equipment and the timing are not well known.	No, detailed analyses have not been performed to address a prolonged event. Limited calculations to support the PRA are available.	No, this is a beyond design basis event and so is not covered in the SAR. Limited information available in the PRA.	Will attempt to derive a realistic scenario based on limited operator expectations and information from PRA.

D.3.2 Understanding the Loss of Service Water Event

Plant Design

This BWR plant, as with many BWRs, has four service water systems that are relevant to this event. These are:

(1) A normally running closed component cooling water (CCW) system that cools recirculation pumps, reactor water cleanup coolers and heat exchangers, fuel pool heat exchangers, and the control rod drive (CRD) pump oil coolers.

(2) A normally running turbine building closed cooling water (TBCCW) system that cools most loads associated with balance-of-plant equipment, including various heater drain pumps, condensate and condensate booster pumps, main feedwater (MFW) pumps, main turbine lubrication oil and other coolers, generator primary water coolers, isophase bus and exciter coolers, hydrogen coolers, and service and instrument air compressors.

(3) A normally running plant service water (PSW) system, which serves as the normal ultimate heat sink and cools CCW, TBCCW, mechanical vacuum pump and steam jet air ejector coolers, drywell chillers, emergency safeguards (ESF) electrical switchgear room coolers, and various other plant chillers, among other equipment. It can back up most of the loads served by the standby service water (SSW) system (see below).

(4) A SSW system, which is designed to be the ultimate heat sink for loads during a loss-of-coolant accident (LOCA) or offsite power loss (which if lost, causes loss of the other three systems above). These include diesel generators, ESF electrical switchgear room coolers (backup to PSW), all emergency core cooling system (ECCS) room coolers, reactor core

injection cooling (RCIC) system room cooler, residual heat removal (RHR) pumps and heat exchangers and room coolers, control room cooling units, fuel pool heat exchangers (backup to CCW), CCW, drywell chillers (backup to PSW), and the service and instrument air compressors (backup to TBCCW).

While the specific ways to lose all service water will not be investigated in this step, it is observed that a loss of offsite power coincident with a common mode or other catastrophic failure of SSW provides one logical way that a total loss of the ultimate heat sink is possible. By virtue of the loads involved, the following represents a summary of the key potential effects of such a loss if it is not recovered following a prolonged period of time:

- loss of the balance-of-plant, including its isolation (i.e., main steam isolation valve closure on loss of condenser) with concurrent reactor trip
- eventual heatup of all the mitigating loads that are used to provide continuous core cooling and other mitigating functions (e.g., power, pumps, heat exchangers)
- various room and other area heatups such as the fuel pool, control room, drywell (containment), and the suppression pool
- loss of service and instrument air pressure throughout the plant
- may induce recirculation pump seal LOCAs due to the inability to cool the seals, resulting in a primary system makeup demand (albeit probably a small demand).

In summary, from the plant design standpoint, the dependencies on service water are great and a total and prolonged loss of the ultimate heat sink is a particularly challenging event.

Procedural Guidance and Related Operator Expectations

Besides the emergency operating procedures (EOPs), which will be discussed later, there are four procedures (which will also be discussed later) that specifically address individual losses of any one of the four service water systems (for SSW, the procedure addresses only losses of any one of the three SSW loops). The operators are trained periodically in the use of these procedures for short-term simulated losses and hence this training and the actions specified by these procedures largely define the expectations of the operating crew. In a total loss of ultimate heat sink, the operators would be carrying out, not only these procedures, but also the EOPs in parallel once the plant is tripped, in an effort to ensure that all plant critical functions (reactor power, reactor vessel level, containment conditions, etc.) are maintained.

The four procedures provide the symptoms (alarms and indications) used to recognize the loss, and can generally be described as requiring the operators to shut down or trip unnecessary loads and use alternative equipment or trains if possible, including alternately running equipment to extend its operation. More on these procedures and the EOPs can be found in Section D.5.4.

PRA Information

The PRA is among the best information sources available to gain insights as to a likely scenario progression. The base case scenario described in the next subsection is largely based on the PRA information and so that information will not be repeated here. However, two key elements from the PRA are particularly worth noting:

(1) The mitigating equipment for this event, with the exception of the diesel generators, heat exchangers, and similar devices (e.g., RHR heat exchangers for shutdown cooling, room air units), will operate continuously for at least a short period of time (at least 1/4 to 1/2 hour or longer) once it is started, depending on the size of the load and how continuously it and other service water-shared loads are needed. In other words, few components will fail almost immediately after they are started as a result of the loss of service water. This fact allows, for instance, for pumps to be run for a few minutes and then shut down, thereby performing an important function for a short period of time such as maintaining reactor pressure vessel (RPV) level. The diesel generators, however, are a counter example to this because they will fail in a potentially irreparable manner in just a few minutes without service water cooling.

(2) It is estimated that in about 4 hours, most areas of the plant (as a result of loss of room cooling) as well as the equipment throughout the plant (e.g., that requiring direct cooling such as pump seals) will be operating in temperatures that put the continued functioning of the equipment in serious jeopardy.

D.3.3 The Base Case Scenario

The possible scenarios in a prolonged loss of ultimate heat sink are dependent on a variety of factors not least of which are the specific operator actions regarding what equipment is used and for how long, as well as what equipment is secured during various times throughout the event. The following, however, highlights what is believed to be a reasonable chain of events which at a general level is a sufficient description of a base case and realistic plant and operator responses to a prolonged loss of service water. This summary and the accompanying representations of the key parameter indications observable to the operators shown in Figures D.1 through D.6 provide the expected "signature" of the event and indicate what the operators are likely to need to do as the scenario progresses. This progression does not include additional complexities (i.e., deviations) beyond those directly caused by the event.

- Initial Condition: The plant is operating at full power when a loss or degradation of service water occurs. This could happen abruptly due to events such as a loss of offsite power followed by complete failure of SSW. Degradation of service water over time could occur due to events such as valve or pump malfunctions or a breach in the PSW system, followed by a failure in SSW due to ice buildup in the intake structure or traveling screens (which could serve as a common mode failure for both PSW and SSW). Depending on the specific nature of the event, initial cues of multiple problems in the service water system (in CCW, TBCCW, PSW, SSW) may include low header pressure, signs of automatic starts of backup service water pump trains, and low surge tank levels, among others. Alternatively, the first

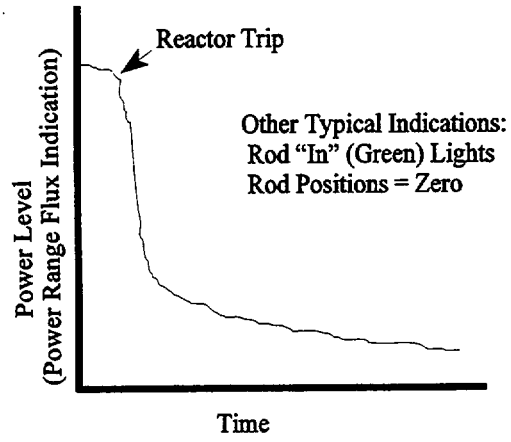


Figure D.1 Power Level vs. Time

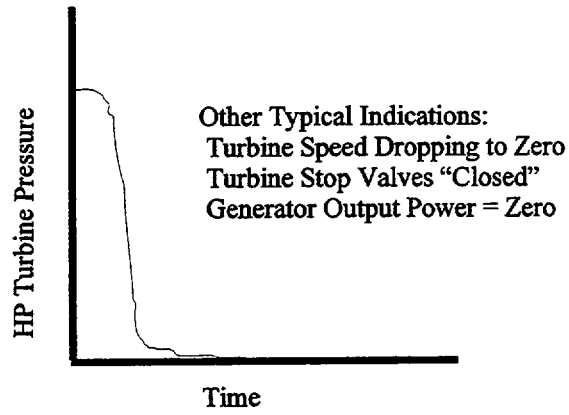


Figure D.2 Turbine Pressure vs. Time

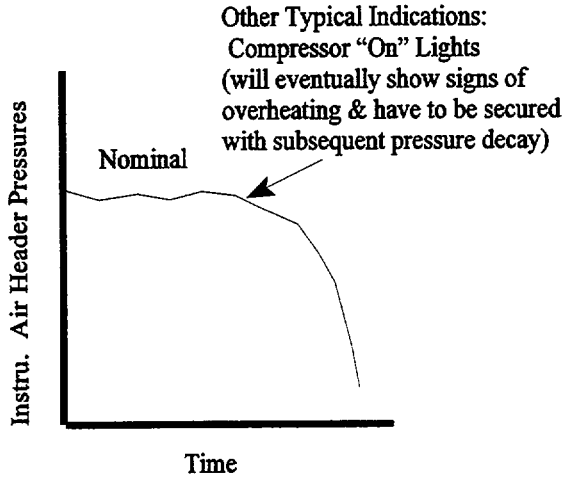


Figure D.3 Instrument Air Pressure vs. Time

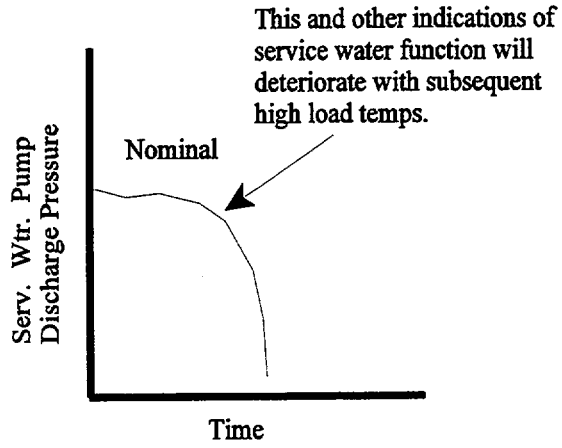


Figure D.4 Service Water Pressure vs. Time

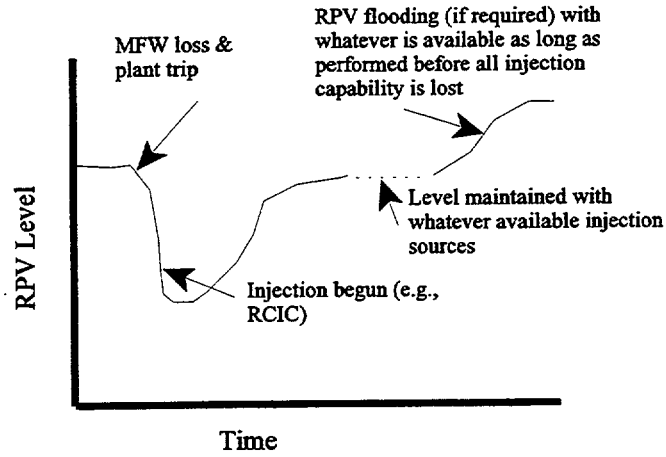


Figure D.5 RPV Level vs. Time

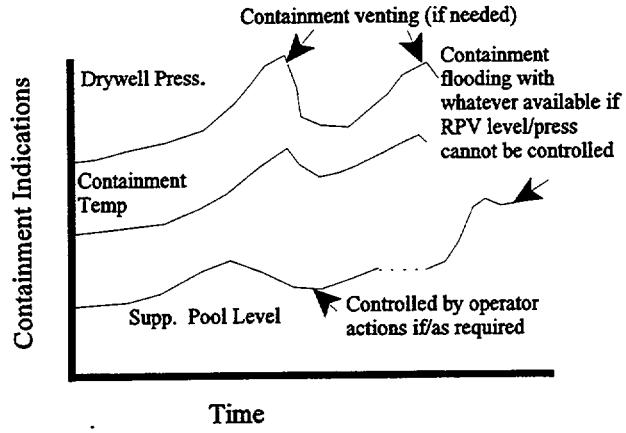


Figure D.6 Containment Conditions vs. Time

cues may be high-temperature alarms on the larger instrumented loads (e.g., recirculation pumps), as well as isolation alarms such as reactor water cleanup isolation or fuel pool heat exchanger isolation. The specific sequence of events cannot be predicted beforehand because it largely depends on the specific faults leading to the total loss of service water. However, and especially in a slowly degrading type of event, the operators will start hearing alarms and seeing indicators of various equipment problems that at first may not seem related or directly attributable to loss of service water. Some degradation of functioning equipment may occur before a plant trip finally results, either automatically or manually by the operating crew.

- Depending on what symptoms appear before the plant trip, the operating crew may already have begun following the steps in one or more of the four procedures for abnormal service water, including securing affected equipment, beginning to troubleshoot the nature and possible sources of the trouble, and eventually manually scramming the plant if required and if an automatic trip has not yet occurred. By the time of the trip, the operators may or may not have yet associated all the symptoms with the common problem of service water cooling.

- The larger loads and the associated service water systems that serve them are likely to develop the initial signs of degradation that finally require equipment shutdown and cause a corresponding plant trip. These are the recirculation pumps as well as all the many loads associated with the balance-of-plant and cooled by the PSW/TBCCW systems. For the base case scenario, the balance-of-plant is isolated either automatically or manually (main steam isolation valves (MSIVs) close) very early in the event (i.e., at or shortly after the plant trip) and all subsequent plant response is based on responding to an isolation-type transient with safety relief valve discharge to the suppression pool serving as the initial heat sink path for core decay heat.

- With plant trip, the operators enter EOP EP-2, RPV control, and by following EP-2 and other automatic and trained responses, they watch for and respond to, as necessary, the following plant conditions (not necessarily in order of priority) as the scenario progresses:

  (1) Reactor power decreases nominally following the reactor trip, as evidenced by the typical indicators and power (flux) time history shown in Figure D.1.

  (2) The turbine trips and the generator load is dropped, as evidenced by the typical indicators and turbine pressure time history shown in Figure D.2.

  (3) One possibility is that all electric buses continue to operate (including required bus transfers) and appear normal, based on breakers indicating "closed," available bus voltages and related indicators that are nominal; and expected operating loads operating as evidenced by current, flow, and similar readings. If the nature of the event has caused an automatic diesel start and there is evidence of lack of cooling to the diesel such as that due to lack of SSW operation, the diesels are supposed to be shut down quickly to protect them. Alternatively, loss of normal power could be a contributing factor to the total loss of service water. In this case, normal bus voltages and currents will drop until and if an attempt is made to run the diesels to restore power. Running the diesels without cooling presents a problem to be discussed later.

  (4) Instrument air, a support system, should be available for a short time, as evidenced by no change in header pressures shown in Figure D.3 and appropriate compressor "on" lights. This is because the compressors should only need to operate intermittently and the heatup of the TBCCW will require a little time to overcome thermal inertia. However, without compressor cooling, compressor failure or shutdown is expected and air pressure will degrade at a rate dependent on the leakages in the system and the demands for air.

  (5) As already alluded to above, service water systems are checked for signs of proper functioning, e.g., pump lights are "on," pump discharge pressures remain nominal over time, and service water load temperatures are nominal. These systems are likely to be already showing signs of trouble as discussed above and illustrated by Figure D.4. Some equipment may have already been secured by the operators. These indicators will continue to show signs of degradation as the scenario proceeds.

  (6) RPV level goes through a time history response typical of that shown in Figure D.5. This history is indicative of a loss and isolation of the balance-of-plant, including failure or shutdown of feedwater with early automatic or manual vessel level restoration via RCIC and/or the high pressure coolant system (HPCS). If a loss of offsite power is part of the event, HPCS operation will likely need to be interrupted or prevented due to a lack of cooling to the HPCS diesel. Safety relief valve (SRV) demands will occur to relieve pressure in the RPV, and pressure and level will be manually controlled by the operator as necessary.

(7) Containment conditions soon react to the loss of drywell cooling and the ineffectiveness of any attempts to cool the suppression pool via RHR due to the degrading service water conditions (see Figure D.6). Injection to the reactor vessel causes, through SRV operation, a rise in the suppression pool level and temperature. These containment conditions cause the operating crew to enter another EOP EP-3, containment control, in an attempt to keep these parameters within acceptable ranges. In the long term, this will not be possible and manual emergency depressurization of the primary system is called for. If or as conditions deteriorate, and once the containment pressure exceeds 20 psig, containment venting is to be performed.

(8) Low-pressure injection systems as well as high-pressure systems are used as necessary to maintain RPV level or flood the RPV if called for, as shown in Figure D.5. Each, however, is subject to failure eventually because of many conditions, depending on the specific system. These include rising suppression pool temperature, rising containment temperature and pressure, high room temperatures (including switchgear equipment), etc.

(9) Depending on the ability of the operating crew to alternate injection trains and extend their usefulness without damage, alternative injection systems may also have to be used to maintain RPV level or flood the RPV as shown in Figure D.5. Firewater lineup into the RPV, which requires local action over about an hour, can be particularly useful because it is independent of the loss of service water. However, without the ability to maintain service and instrument air compressors and with the eventual rise in containment pressure, maintaining SRV operation to keep the RPV pressure low for firewater and other low-pressure injection is jeopardized.

(10) Should the accident progress to the point that the ability to maintain RPV level and/or SRV operation is in serious doubt, containment flooding is started with whatever injection sources may be available (see Figure D.6).

(11) No radiation indicators or alarms are present, at least early in the scenario.

(12) Operators will be noting adverse indicators or alarms associated with ventilation problems and high temperatures in various rooms as well as the fuel pool.

- All the while, ultimate heat sink restoration will be being attempted.
- The technical support staff will likely be convened and the emergency plan enacted.
- At any time when the ultimate heat sink is restored and plant conditions can be restabilized, continued cooldown of the plant and shutdown of unnecessary equipment occurs.

Note that in the base case scenario, operating crew decisions and actions take place on a continuous basis in an attempt to deal with the deteriorating conditions. Some actions may be required

immediately, such as shutting down diesel generators before they are damaged. Most occur over time as decisions are made regarding what equipment to use and for how long. This is a "balancing act" between maintaining adequate core and containment conditions for as long as possible vs. shutting down or securing equipment to avoid its being damaged (perhaps irreparably).

D.4 Step 4: Define Human Failure Events (HFEs) / Unsafe Actions (UAs)

Based on the issue as defined in Step 1, part of the purpose of this analysis is to identify what the more likely HFEs/UAs may be in light of the changing plant conditions during the scenario progression. Hence, the HFEs/UAs cannot be defined a priori, but instead will be a product of this analysis. However, in general, the potential HFEs/UAs of interest all involve potential failures of the operating crew to "control" individual equipment items in a way that preserves their functionality for as long as possible and makes the best use of limited water, power, and compressed air resources so that the necessary safety functions can be maintained for as long as necessary. Actions such as securing systems from automatic control, manually initiating or backing up necessary automatic functions, stopping running equipment when considered necessary, operating equipment in unusual configurations, etc., are among the many examples of operator actions that may need to be performed if the loss of heat sink exists for hours. For example, operators may need to shut down diesel generators, start/stop/swap various injection trains to avoid serious overheating, disable undesired system starts, manually perform functions such as emergency depressurization, bypass automatic reconfiguration of equipment such as HPCS to the suppression pool (to avoid this "hot" injection source of water), etc.

A review of Tables 9.6 and 9.7 reveals that every functional failure mode category and example HFE may be applicable to the required operator actions in this scenario. This analysis serves to identify which HFEs/UAs appear to be more likely and under what circumstances their likelihoods appear to be the highest.

D.5 Step 5: Identify Potential Vulnerabilities in the Operators' Knowledge Base

Given the already challenging nature of the scenario described, this step is the first involving the identification of those complexities associated with the base case scenario that introduce contexts that can make HFEs/UAs likely. While some deviations from the base case scenario may be examined as a result of uncertainties in the specific accident progression, deviations as a result of random equipment failures will not be addressed in this analysis. Consideration of characteristics of the scenario, formal rules and procedures, informal rules, operator tendencies and biases, potential procedural difficulties, and potential timing and workload are among the issues involved in identifying such complexities and deviations. This step reviews potential vulnerabilities with regard to these issues that may make HFEs/UAs likely.

D.5.1 Potential Vulnerabilities in Operator Expectations for the Scenario

Examination of Table 9.10, which addresses event types and related potential operator vulnerabilities, results in the following observations relevant to this analysis for this plant.

- The loss of service water event fits a class of events that are rare and not even anticipated during the life of the plant (i.e., beyond design basis). While there have been precursor events at a few plants where service water became severely degraded or even lost, it was recovered before a serious event ensued. Therefore, training is performed infrequently and only involves partial losses of individual service water systems. In addition, the simulated scenarios typically only cover the first half-hour or less in the accident progression to ensure that the symptoms are properly identified and diagnosed, and that the early required actions are performed. Attention is not spent on training for a prolonged and total loss of the ultimate heat sink, which would also be a difficult event to simulate due to simulator limitations. There are therefore only limited expectations by the operating crew as to what such a scenario looks like and the expected response of plant equipment and indicators. As such, the scenario represents a mismatch between expectations on the part of the crews and the existence of the scenario itself.

- Based on information presented in Table 9.10 as applicable to a loss of service water scenario, potential vulnerabilities could include:

  - unfamiliarity as to what to expect and therefore how to plan ahead in such a scenario
  - places where the procedures and other rules may not be appropriate or adequate
  - limited guidance on how to decide among alternative actions
  - the potential to have to coordinate among people in multiple locations

Based on the above observations, it should be the focus of the next step (Step 6) to identify scenario complexities and characteristics that test the potential vulnerabilities to determine whether HFEs/UAs are likely to occur because of these vulnerabilities.

D.5.2 Time Frames of Interest

As a further insight into the potential for HFEs/UAs to occur, four time periods in the scenario can be identified relative to potential operator influences. These are summarized in Table D.2.

The above summary illustrates that throughout the scenario (even pre-initiator), operators are continually involved in an attempt to first identify and isolate the problem and prevent a trip, and then to respond to degrading conditions throughout the scenario progression. They must also coordinate attempts to identify the source of the loss of heat sink and recover from it. If the event is not recovered quickly, more staff are likely to be called in, including the technical support staff. Emergency plan actions may begin. Environmental conditions will degrade as room areas heat up as a result of the loss of cooling. All of this is likely to result in increasing stress with resources potentially stretched to deal with the varied set of problems. Consideration of these observations about the scenario should be included in the next step (Step 6).

Table D.2 Relevant Time Frames for the Loss of Service Water Scenario

Time Frame	Major Occurrences	Potential Operator Influence
Pre-initiator	Alarms or indicators begin to show signs of trouble due to service water degradation Some equipment malfunctions may begin	Begin troubleshooting problem, attempting to find and address source of problem. Operators begin shutting down seriously affected equipment immediately.
Initiator	Loss of MFW and balance-of-plant Reactor scram or turbine trip MSIV closure now or soon after	The plant trip may occur automatically or the operators may trip the plant, depending on their observations regarding the equipment being affected.
0 - 10 minutes	Auto equipment responses occur (e.g., RCIC, HPCS start to restore level) Diesels may start if high drywell pressure present Containment isolation may occur now or soon	Operators verify or back up initial plant responses (particularly those that are automatic, such as lowering power level) per EOPs. If operators are aware of equipment high temperature or service water problems, they may need to quickly shut down or secure or even prevent some equipment starts.
>10 minutes	Equipment degradation occurs over time, room areas heat up, degrading containment conditions develop, etc.; critical safety functions are maintained for as long as possible by operators. If or when heat sink restored, restabilization and cooldown of plant occurs	Operators deal with equipment and plant degradation issues by alternating equipment operation, securing some equipment, using alternative systems, and performing many other actions necessary to respond to the event. Key core and containment cooling actions include maintaining RPV level and flooding it if necessary, emergency depressurizing if and when necessary, attempting to cool containment and venting it if and when are required. All the while, attempts are coordinated to restore service water. Technical support staff is convened and emergency plan commenced if recovery is not quick.

D.5.3 Operator Tendencies and Informal Rules

Many of the operator action tendencies summarized in Table 9.12b apply in this scenario because they describe what the operators will be attempting to do in response to parameter indications. Those actions that are most relevant as the situation continues to degrade, include:

- attempting to restore or augment loss of cooling water
- maintaining RPV level and not letting it decrease too fast or get too low by using various injection systems
- pressure maintaining low with SRVs, vessel vents, etc., especially after emergency depressurization

- attempting to prevent containment conditions from getting "too high" via the action tendencies shown

- preventing irreversible equipment damage by shutting down/securing/alternating operation whenever possible.

Using examples from the Table 9.13, at this plant a particularly relevant informal rule is that there is a strong tendency to follow and "believe in" the procedures. Experience has shown them to be capable of handling at most any situation, even though this scenario has not been trained for or simulated.

These tendencies, while good, do provide somewhat conflicting directions as to how the operators are to proceed. In particular, for this scenario, the last tendency listed above (prevent irreversible damage to equipment) is somewhat in conflict with the other tendencies to use the equipment to maintain safety functions. Specifically, while the four procedures for abnormal service water generally direct equipment to be shut down, the EOPs direct the use of mitigating equipment to the extent possible. These procedural and tendency differences could create so-called "double-binds" where the operators must choose among undesirable alternatives. Resolution of these issues as they arise is a potential vulnerability since the event will test the understanding of the crew as to the status of the plant and equipment; they will have to rely significantly on their cognitive skills rather than the skills involved in simply following procedures. In this case, the procedures conflict somewhat.

D.5.4 Evaluation of Formal Rules and Emergency Operating Procedures (EOPs)

This evaluation looks for vulnerabilities associated with ways the emergency operating procedures (EOPs) and other formal rules may lead operators to HFEs/UAs. In this case, the EOPs and the four procedures provide the primary inputs that will guide the operators' actions when responding to a loss of service water event. This examination is developed by tracking those portions of these procedures that are most germane to the scenario.

Figures D.7 through D.9 display in very simplified flowcharts the major actions called out by the various procedures once the scenario progresses past the initial power reduction, which is assumed to be successful. Note that these flowcharts are not meant to duplicate the procedures. However, they do highlight the most significant cues called out by the procedures and the actions to be taken. In particular, the hexagon shapes represent places where equipment is terminated. These and other places in the procedures represent possible vulnerabilities where it may be more likely for the HFEs of interest to occur, thereby jeopardizing the scenario outcome.

Review of the above procedures for potential vulnerabilities that might lead to HFEs/UAs suggests the following observations:

- From an overall perspective, and as already mentioned in Section D.5.3, some potential conflicts are set-up among the procedures. The abnormal service water procedures call for shutting down equipment, while the EOPs require equipment to be used to maintain safety functions.

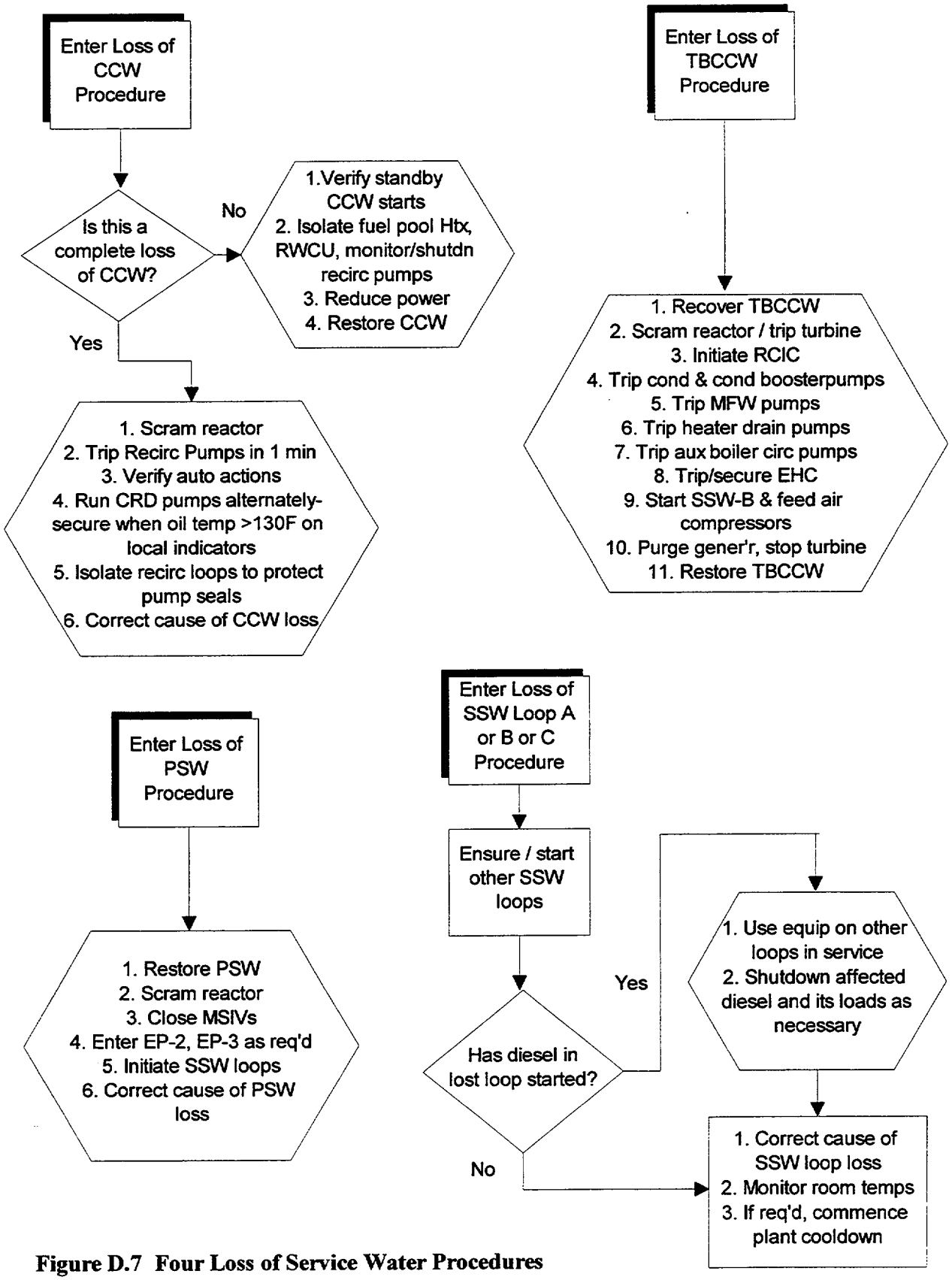


Figure D.7 Four Loss of Service Water Procedures

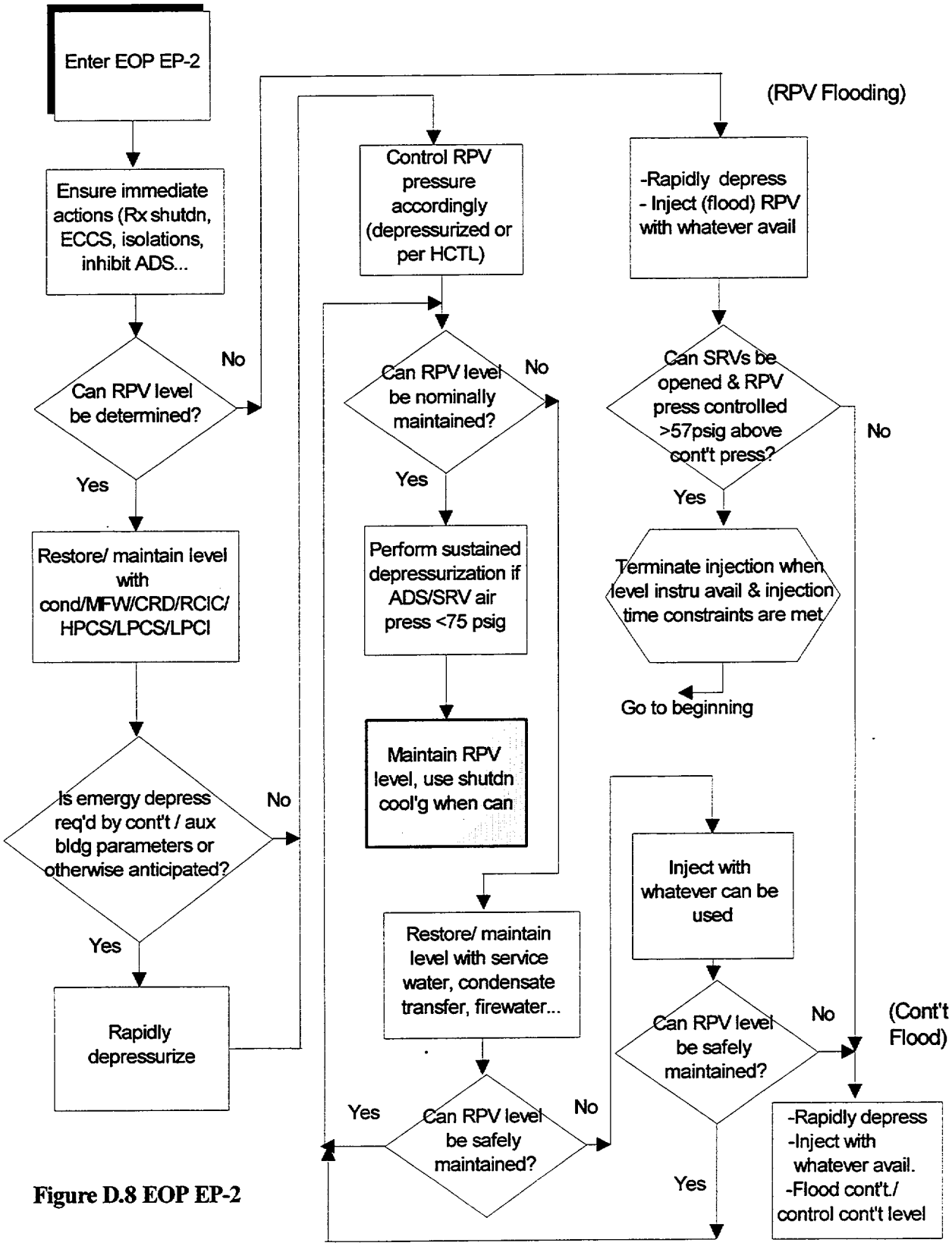


Figure D.8 EOP EP-2

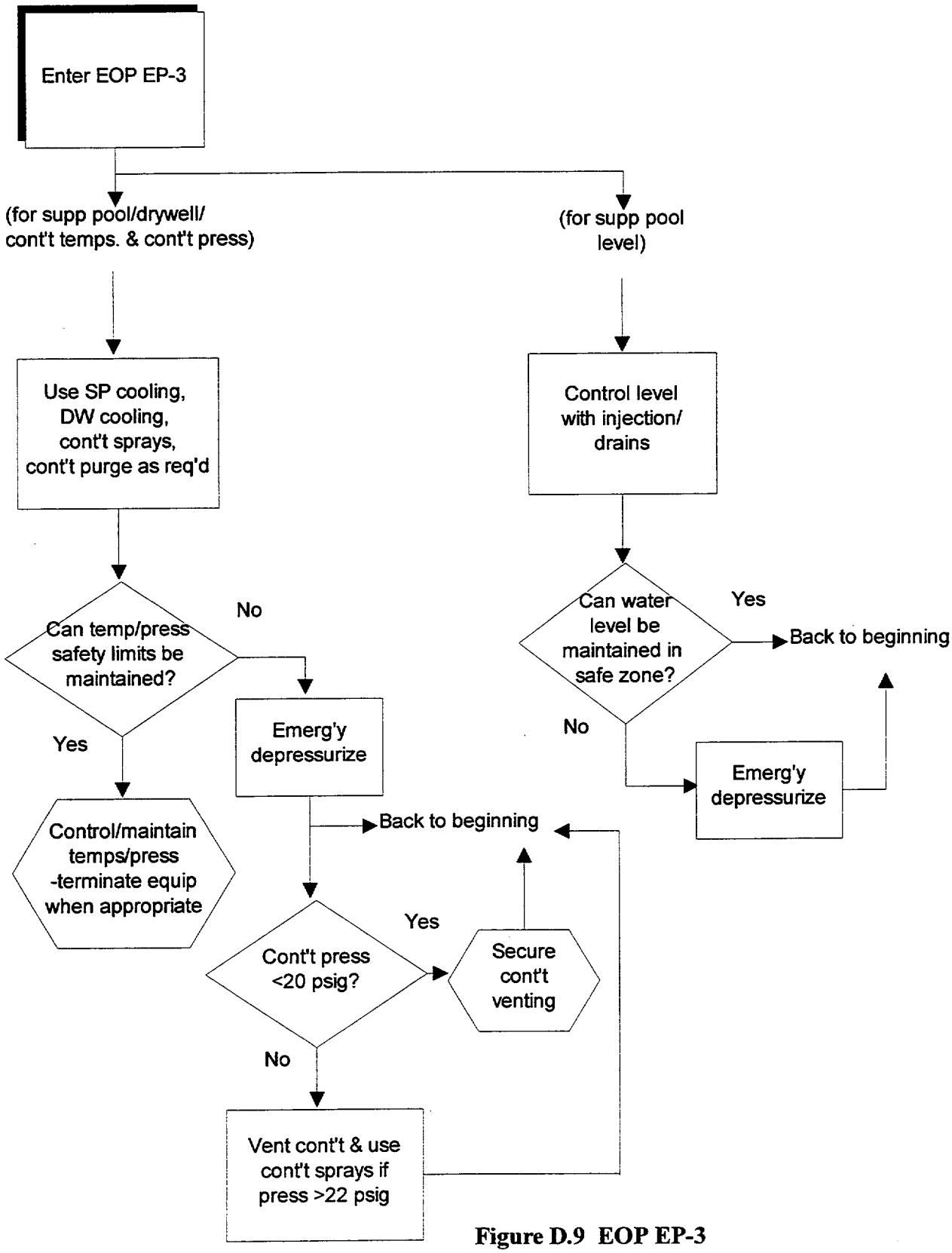


Figure D.9 EOP EP-3

- No specific procedure exists for loss of all three loops of SSW; thus the operators will have to cognitively extend the use of the Loss of SSW abnormal procedure, while also attempting to follow the EOPs.

- If a loss of offsite power were involved and SSW were to completely fail, operators would be presented with the choice of shutting down diesels to protect them and forcing a station blackout, or running one or more diesels to power equipment (preferred actions are not indicated in procedures).

- If diesels start (e.g., from high drywell pressure) with offsite power available, diesel shutdown should be performed but must be done quickly to avoid irreparable damage.

- Failure to shut down or, if appropriate, extensively cut back the use of running or automatically started equipment during the initial and later phases of the accident could damage the equipment so that its later use cannot be relied upon. Indications of impending equipment damage may occur late or not at all, creating ambiguous criteria as to when to start or restart equipment, how long to run it, and when to shut it down.

- Restoring or maintaining RPV level will be the likely first safety function challenge for the operating crew and will require quick decisions and unambiguous communication among the crew, as to which equipment to start and let run (and for how long), and which equipment to shut down or secure, even if automatically started. Failure to maintain this function could lead directly to core damage.

- Responding to higher containment temperatures and pressures will also be an early challenge for the operating crew and will also require unambiguous communication among the crew as to which equipment to start, when, and for how long; and which equipment to shut down or secure even if it was automatically started. Whether systems that can cool either the core or containment (e.g., RHR), depending on the alignment, should be preferably used for core cooling or containment cooling may also be an issue for which no procedural guidance is provided.

- Air pressure will likely deteriorate if the compressors are not or cannot be run by the operators periodically. This could severely hamper the ability to emergency depressurize and maintain depressurization, especially if SRV operation is not managed so as to avoid using up any backup or bottled air sources. Operators will need to be aware of this issue because loss of the ability to depressurize and maintain pressure control could lead to core damage.

- Failure to defeat unwanted or undesirable alignments such as RCIC switching to the suppression pool for suction (pool temperature will get high due to lack of RHR-SSW cooling) could result in equipment damage and the inability to operate the equipment, if needed later.

- Failure to take other desirable measures such as using portable room cooling, refilling the condensate storage tank if needed, dropping unnecessary electrical loads, and arranging a temporary means for cooling water to vital loads could cause losses of air, water, and power (consumables) needed to respond to the event.

- As a final and general observation, having performed this review, it appears that many of the characteristics of the scenario are similar to a station blackout (SBO) for which this plant has a procedure; by carrying it out, the plant can supposedly cope for up to at least 4 hours. However, in this case, some or all of the power may be available and so the operator needs to be more involved with shutting down equipment to "save it for later" if needed. In many ways, it seems the SBO procedure would be applicable, but with modification. As of now, no specific guidance is available as to equipment priorities, timing of desirable actions, other unusual actions to take, etc.

D.5.5 Summary of Potential Vulnerabilities

Based on the information from this step, Table D.3 summarizes potential vulnerabilities that may make HFEs/UAs by the operating crew plausible. These are addressed further in Step 6.

D.6 Step 6: Search for Deviations from the Base Case Scenario

The scenario being analyzed already represents a significant deviation from operating crew expectations; in fact if it were to occur, disbelief could be an initial natural reaction. Without additional complexities, such a scenario is already quite challenging and in light of the identified vulnerabilities, offers a number of instances for the crew to perform unsafe acts. Because of this, deviations from the base case scenario considered in this step will generally not include such issues as random equipment faults or indicator failures because it does not seem these would be necessary to make the scenario sufficiently error forcing. However, potential deviations of the scenario itself and how it might progress will be considered in the following searches to see if certain circumstances can lead to strong error-forcing contexts.

D.6.1 Search for Initiator and Scenario Progression Deviations from the Base Case Scenario

The search for possible scenario deviations is begun by first considering deviations in the initiating event itself as well as in the scenario as a whole. In this case, a useful approach is to apply guide words typical of hazard and operability analyses to investigate differences in the way the initiator or scenario might proceed.

Table D.4 demonstrates the possible deviations that have been considered in this search. The types of initiator or scenario deviations that seem to have the most potential for inducing HFEs/UAs involve a somewhat slowly degrading type of initiator that may provide diagnosis problems at first, while at full power with the highest heat loads. The possibility of a demanded SRV sticking open, thus, quickening the necessary responses and placing a greater demand on RPV injection, is also of particular interest. The combination of these characteristics may make for the most challenging event and it is this combination that is reviewed further in Table D.5.

Table D.3 Summary of Potential Vulnerabilities for Loss of Service Water

Consideration	Observation	Vulnerability/implication
Training, experience, expectations	Has never happened (though some precursors at other plants); seems impossible	Disbelief (mismatch from expectations)
	Limited training on lesser losses of water cooling systems individually. No training on prolonged total loss (beyond design basis accident)	Unfamiliarity Limited procedural and other guidance Multiple location coordination required
Timing considerations	Signs of trouble and equipment malfunctions may occur for a time before trip	Failure to diagnose cause early could affect future decisions Failure to shut down affected equipment could cause additional problems
	Diesels may start	If need emergency power, there is no specific guidance as to shutdown vs. operate any of them
	Equipment and room areas will degrade over time	Need to intervene considerably; trying to maintain safety functions with limited equipment use and no specific procedural guidance
Tendencies or informal rules	Tendencies exist to recover and maintain safety functions and prevent irreversible equipment damage	For this scenario, tendencies oppose each other, requiring careful balance
	Crews follow procedures	Abnormal procedures tend to oppose needs of EOPs. Clear procedural guidance not available
Formal rules/procedures/EOPs (for observations not covered above)	Involves a total loss of service water, including all SSW	No specific procedural guidance for loss of all SSW
	Decisions as to what equipment to run, stop, when, and how long	No specific guidance. Will require strong coordination and communication
	Consumables (air, water, power) in jeopardy long term	Must manage and anticipate without specific guidance
	Need to take other desirable actions and prevent undesirable equipment alignments or starts	Limited guidance
	Some similarities with SBO	SBO procedure maybe helpful, but needs modification "on the fly"

Table D.4 Loss of Service Water Initiating Event / Scenario Deviation Considerations

Guide Word	Possible Physical Deviation	Significance	Carry Forward in the Analysis?
No/not/never	Initiator - N/A Scenario - N/A	Relative to the initiator or scenario, "no" loss of service water eliminates the initiator and so there is no scenario. Use of this guide word is not applicable.	No.
More/early/ quicker/ shorter	Initiator - abrupt loss Scenario - coincident LOCA requires quicker responses	The base case scenario did not give the specifics of the initiator. The loss could be total and abrupt. It is not clear that such a loss changes the time or nature of the response significantly enough to be a concern, with the exception of requiring a quick shutdown of the diesels. A total abrupt loss may be easily identified based on the numerous alarms that would all come in at once. The demands on the plant and operator response will be the quickest if the pre-initiator plant condition is full power with greatest heat loads. A simultaneous LOCA or similar event would also "quicken" the scenario, but the coincident probabilities are considered too low, with the possible exception of a stuck-open SRV or RCP seal LOCA.	See below. Also, significant RCP seal LOCA not likely and should be isolated by procedure, anyway. Stuck-open SRV adds an additional challenge for earlier and more continuous injection.
Less/slower/ longer/late/ partial	Initiator - Service water is not totally and abruptly lost initially, but is only partially or slowly lost over time Scenario - low power level and heat loads	For the initiator, this is a possible situation in which it may be harder to detect and identify the source as well as the extent and nature of the problem. Such a situation might delay diagnosis of the problem and responses to the effects. The scenario and related degradation could occur slower, especially at low power levels and corresponding heat loads.	Combination of slower or harder to detect initiator while at full power seems to provide the most challenging event.
Reversed/ repeated/as well as	Initiator - Service water is apparently restored, but it is still not sufficient or is lost again (repeated) Scenario - N/A	For the initiator, this is a possible situation that could add confusion as to the extent and nature of the recovery. Such a situation might enhance the chances of operating more equipment simultaneously, only to have to respond again to the repeated service water loss.	No. Probabilistically too less likely overall than above.

Table D.5 Results of the Loss of Service Water Initiating Event/Scenario Deviation Analysis

Possible Physical Deviation	Potential Error Mechanisms Affecting Human Response	Potential Error Types	Further Analysis?
Service water is not totally and abruptly lost initially, but is only partially or slowly lost over time while plant at full power. Recovery is not forthcoming, requiring operators to decide on what equipment to run when, etc. as the situation continues to degrade. A stuck-open SRV during the event places a greater early and continuous demand for injection.	No or smaller change in parameters than expected. (No indication or slower or smaller than expected changes in plant parameters occur at first due to slowly degrading situation.) Starts as apparent simple, "garden path" problem, thereby triggering familiarity or even complacency. [Starts as partial loss of service water (expected) but could degrade and become a total loss and hence more severe] Familiarity and simple expectations about the event need to be overcome if the situation changes. (Situation could start as partial loss and become total loss, perhaps unexpectedly, requiring the situation assessment and response change.) Scenario contains dilemmas and response contains double-binds. (Undesirable alternatives such as stop equipment to "save it" vs. operate equipment to maintain safety functions, both per procedures, may setup delays in the response, reluctance or cautiousness, anxiety and stress.) Scenario has many side effects that take time to develop. (There could be fixation on immediate problems and insufficient planning for what is to come.) Delays in changes of parameters may cause events to be a surprise as there is limited knowledge as to what to expect and when. (Equipment degradation may not be indicated and alarmed right away but be delayed.) Scenario may require high tempo/multiple tasks at times adding to anxiety and stress. (Potential for simultaneously indicating problems and some necessary quick responses such as shutting down diesels could add to anxiety and stress.)	May take no action or delayed action to prevent further degradation of service water or respond to its effects due to lack of awareness, at first, as to nature of problem. Could believe situation has stabilized with some service water flow and thus be caught off guard when total loss occurs; potentially missing some necessary immediate actions such as shutting down diesels or loads. Wrong or inappropriate actions could be taken or needed actions could be taken too late, regarding which equipment to operate or shut down, when to do it, for how long. Could result in unnecessary equipment damage or safety function degradation. Note that the overall strategy decision as to how to respond could be an important and potential error (e.g. fill vessel and depressurize early vs. maintaining status and waiting for procedural cues). Insufficient planning may exist as to what may happen next, as well as in the longer term, so that best response and use of resources (equipment, consumables, staff) is not achieved. Anxiety and stress, should scenario seriously degrade, could disrupt coordination efforts and challenge communication among staff so that actions are taken by individuals without full knowledge of entire crew.	Yes. Should carry forward. Many error mechanisms are potentially triggered by this possible scenario.

Table D.5 summarizes more specifically how the above combination might trigger relevant cognitive processes, error mechanisms, and related error types based on a review of Tables 9.15a and b as well as 9.16a and b, in ways that might induce HFEs/UAs of concern. For the possible physical deviations being considered, the contents of Tables 9.15a and b and 9.16a and b that are the most relevant are shown in the second column of Table D.5. The third column of Table D.5 summarizes the potential errors (HFEs or UAs) that could occur given the general error types provided in those tables.

D.6.2 Search of Relevant Rules

This portion of the analysis examines whether unsafe acts could be induced as a result of deviations from the base case scenario so that incorrect procedural guidance or other rules are followed, or the prescribed actions can be applied in ways that would cause HFEs/UAs. Note that while possible deviations could be examined as to the *specific* sequence of events, these are likely to be dependent on the operator actions and may be too numerous to investigate efficiently. So this examination is made considering the overall scenario and not the timing and sequence of specific events and how they might deviate from one another. Besides, the observations made below are generally applicable anyway.

Step 5 resulted in the identification of a number of vulnerabilities that could induce unsafe acts for the scenario as postulated. The vulnerabilities that may directly or indirectly relate to the procedural or other rules followed by the operators can be summarized as:

- there is no specific procedural guidance for loss of all service water
- the four abnormal procedures, the EOPs, and other rules which tend to be followed by the operators potentially set-up conflicts with regard to shutting down equipment vs. operating equipment to maintain safety functions
- operating crews at this plant have a strong belief in the procedures and tend to follow them with little discretion, further setting up a potential conflict as to what extent to follow the abnormal procedures vs. the EOPs.

The scenario itself is considered sufficiently challenging and these vulnerabilities are considered to be sufficiently strong that investigation of further deviations from the base case scenario do not appear warranted, with the exception of the stuck-open SRV, which was identified earlier. Such a deviation quickens the need for injection and may cause a more continuous demand for injection over longer periods of time. This places a greater demand on proper operator response.

Furthermore, the decisions with regard to overall strategies (call them "rules" here) for responding to this event could be critical with regard to how the scenario proceeds. For example, in EOP EP-2, the decision about whether emergency depressurization is anticipated (even though strict requirements are not yet met) could lead to an early transfer of energy from the core to the suppression pool, or a later transfer. Whether to simply control RPV level within certain limits vs.

purposely overfilling the vessel (but which will require longer sustained injection) could lead to very different demands on system operations and hence their potential for damage. Whether to shut down diesels in certain situations provides another case where a strategy decision will have to be made, perhaps quickly. The existing potential ambiguity as to which "rules" (strategies) to follow could significantly affect the scenario progression and outcome.

A review of Table D.5 and the potentially triggered error mechanisms and resulting error types relevant to the scenario listed in that table suggests that these apparent problems with the existing "rules" serve to further support the existence of those error mechanisms and types. The rule problems do not necessarily introduce new error types of their own; they simply make the error types identified in Table D.5 (which are fairly general) more likely. This is an important consideration later in the analysis when consideration is given to the likelihood of making unsafe acts.

D.6.3 Search for Support System Dependencies

This search focuses on ways that deviations as a result of support system failures could further add to the error-forcing context of the scenario. In this case, the event itself already involves the complete failure of a major support system of the plant. Further, the potential effects on other support systems, including air and power, have already been considered in the scenario complexities along with the possible ramifications. These include the potential inability to depressurize and/or control RPV pressure, as well as the diesel start issue and the potential for station blackout.

Other possible deviations (but not simply random independent failures of equipment) involving electrical power could include a loss of offsite power as a contributor to the event as well as temperature-driven failures of electrical switchgear, etc. Such deviations would, in the context of this scenario, simply serve as yet other ways that equipment may fail so that it cannot be used. While loss of offsite power would likely cause more of an abrupt loss of the normally running water systems (CCW, TBCCW, PSW), SSW could still degrade over time, depending on the failure mode(s) and therefore the initiator could still be a slowly developing event. In addition, loss of offsite power will further limit the available equipment choices for the operators, depending on which buses are lost and when.

Furthermore, the loss of efficiency in chiller/heating, ventilating, and air conditioning/unit coolers will result in rising room temperatures. This effect will make the environment in the main control room and other areas of the plant less comfortable. This adverse environment could add to the anxiety and stress of the staff as well as potentially increase the chances of making poor judgments in assessing the situation and carrying out tasks. Some temperature-sensitive electronics, indicators, etc. could also be eventually affected, further hampering operator response in the long term.

As with the relevant rule search, it does not appear that the loss of power or induced loss of room cooling would necessarily create new error types from those already identified in Table D.5, which are defined as sufficiently general (although adverse environmental conditions could be considered to introduce new error mechanisms such as tiring and lack of focus). However, the potential for power losses to more severely limit equipment choices, the additional workload and attention issues

created by losing power and the resulting efforts to get power back, and the adverse environmental conditions are likely to make the generally defined unsafe acts even more likely.

D.6.4 Search for Operator Tendencies and Error Types

This search focuses on the tendencies of the operators and the potential error types as a result of those tendencies. Like the search above for relevant rules, note that while possible deviations could be examined as to the *specific* sequence of events and what the operators would tend to do in those specific circumstances, these are likely to be too numerous to investigate efficiently. So this examination is made considering the overall scenario and not the timing and sequence of specific events and how they might deviate from one another. Besides, in a general sense, the two strongest applicable tendencies will likely govern the operators' overall response regardless of the specific situation; these are the potential conflict of the tendency to want to shut down equipment to avoid damage vs. operating the equipment to ensure safety functions. These tendencies are supported by the operators' tendency to follow procedures which for this scenario, call for response to an unfamiliar event for which they have little training and potential procedural conflicts and lack of specific guidance.

Based on these observations, and keeping the search general in scope, it does not appear that these operator tendencies would create error types different than those already identified in Table D.5, which are defined as sufficiently general.

D.6.5 Develop Descriptions of Deviation Scenarios

Because of the nature of the scenario being examined and the already challenging nature of the event, the above searches have not investigated specific deviations from the base case scenario described in Section D.3. For instance, random independent failures of equipment have generally not been considered during the search process. The searches have, however, considered overall scenario deviations resulting primarily from likely cascading effects of the loss of service water event and provided a better understanding as to the potentially triggered error mechanisms and possible error types (defined in a general sense) that may more likely occur. During these searches, it was found that a stuck-open SRV during the event and the possibility of power losses either as part of the initiator or much later in the scenario would be additional deviations that could increase the need for definitive responses and limit the available equipment that could be used.

Therefore, for purposes of this analysis, a scenario will be examined that is considered to follow that generally described in Section D.3 for the base case, but that includes an early stuck-open SRV. The possibility of losing power at some time in the event (i.e., initially or subsequently due to high room temperatures) will be considered.

For this scenario, a summary of what appear to be the more relevant general types of error mechanisms and types is presented in Table D.6, which is largely duplicative of Table D.5. Based on the information in the table, a list follows summarizing the seemingly most relevant scenario-related HFEs/UAs that might be induced and their general impact on the scenario progression.

Table D.6 Loss of Service Water Scenario Summary

Overall Plant Condition (Scenario)	Potential Error Mechanisms Affecting Human Response	Potential Error Types (HFEs/UAs)
Service water is not totally and abruptly lost initially, but is only partially or slowly lost over time while plant is at full power. Recovery is not forthcoming, requiring operators to decide on what equipment to run when, etc. as the situation continues to degrade. A stuck-open SRV early in the event places a greater early and continuous demand for injection. Offsite power may be lost initially or electrical buses may begin to gradually have problems and load disruptions occur due to high room temperatures in electrical bus rooms.	No or smaller change in parameters than expected. (No indication or slower or smaller than expected changes in plant parameters occur at first due to slowly degrading situation.) Starts as apparent simple, "garden path" problem, thereby triggering familiarity or even complacency. [Starts as partial loss of service water (expected) but could degrade and become a total loss and hence more severe] Familiarity and simple expectations about the event need to be overcome if the situation changes. (Situation could start as partial loss and become total loss, perhaps unexpectedly, requiring the situation assessment and response change.) Scenario contains dilemmas and response contains double-binds. (Undesirable alternatives such as stop equipment to "save it" vs. operate equipment to maintain safety functions, both per procedures, may setup delays in the response, reluctance or cautiousness, anxiety and stress.) Scenario has many side effects that take time to develop. (There could be fixation on immediate problems and insufficient planning for what is to come.) Delays in changes of parameters may cause events to be a surprise as there is limited knowledge as to what to expect and when. (Equipment degradation may not be indicated and alarmed right away but be delayed.) Scenario may require high tempo/multiple tasks at times adding to anxiety and stress. (Potential for simultaneously indicating problems and some necessary quick responses such as shutting down diesels could add to anxiety and stress.)	May take no action or delayed action to prevent further degradation of service water or respond to its effects due to lack of awareness, at first, as to nature of problem. Could believe situation has stabilized with some service water flow and thus be caught off guard when total loss occurs; potentially missing some necessary immediate actions such as shutting down diesels or loads. Wrong or inappropriate actions could be taken or needed actions could be taken too late, regarding which equipment to operate or shut down, when to do it, for how long. Could result in unnecessary equipment damage or safety function degradation. Note that the overall strategy decision as to how to respond could be an important and potential error (e.g. fill vessel and depressurize early vs. maintaining status and waiting for procedural cues). Insufficient planning may exist as to what may happen next, as well as in the longer term, so that best response and use of resources (equipment, consumables, staff) is not achieved. Anxiety and stress, should scenario seriously degrade, could disrupt coordination efforts and challenge communication among staff so that actions are taken by individuals without full knowledge of entire crew.

Based on the above information, scenario-related "general" HFEs/UAs more likely to be potentially induced include the seven listed below.

The following are potential HFEs/UAs related to *certain actions of the crew*:

(1) *Diagnose initiator. Failure to diagnose source and full scope of the initiating event early.*

Unawareness or misdiagnosis of the source (loss of service water) and scope (eventual total failure) of the event could result in operators not shutting down unnecessary loads or swapping or alternating equipment, at least at first, as the EOPs are followed. This could result in irreparable damage to equipment items, making them unavailable for later use and thereby more severely limiting the equipment options later in the scenario. If the diesels were involved and not shut down quickly, the plant could experience a station blackout depending on the condition of offsite power. If too much equipment becomes failed, safety functions may not be able to be maintained and core or containment damage may result.

(2) *Diesel management. Failure to properly respond to diesel generator starts initially or later in the scenario.*

It is not clear ahead of time as to the appropriate response because it likely depends on the condition of other power sources, which loads are needed and when and for how long, etc. As stated above, the possibility of entering a station blackout, loss of safety functions, or irreparable damage to the diesels could result.

(3) *Equipment management. Shut down or secure equipment to protect it at an inappropriate time when it is vitally needed, fail to prevent startup of equipment (or manually start it) when it is not needed, fail to shut it down before damage occurs to the equipment, or fail to prevent undesirable alignments that may increase damage to the equipment.*

This is a potential issue throughout the scenario and requires cognizance of the status of overall plant conditions and individual equipment throughout the scenario. Depending on the overall strategy of the operating crew, maintaining a level of redundancy of mitigating equipment for all safety functions would be most desirable. Inappropriate responses of this nature could cause the loss of equipment needed to mitigate the event and jeopardize the safety functions.

(4) *Consumables management. Use equipment in ways that cause the loss of consumable resources.*

Water for injection, compressed air, and electrical power are resources needed to mitigate the event. For example, operating compressors until they fail or using SRVs too many times with backup air or nitrogen could lessen the chance of successfully depressurizing and controlling pressure when required. External water sources will be cooler than the suppression pool as a suction source and thus actions taken to preserve or replace their contents may be desirable. Nonrecognition of the desire to drop unnecessary electrical loads and use portable room cooling for electrical bus rooms could result in later problems with electrical power. If not used and protected wisely, loss of these consumables could lead to the inability to use mitigating equipment at a vital time, thereby causing loss of safety functions.

The following are potential HFEs/UAs that can affect the *overall response of the crew* and thereby contribute to or lessen the chances of the HFEs/UAs listed above:

(5) *Adopt an overall poor strategy or plan at the beginning of the scenario.*
The overall crew strategy or plan as to how to respond to the event should be decided early and consider the best way to save equipment and consumables while meeting the needs of the safety functions. For instance, overfilling the RPV early will allow more time for later responses (it will take longer for the vessel level to drop to undesirable limits), but will require more continuous use of equipment early in the scenario. A poor strategy (probably one involving too much maintenance the status quo and not anticipating later needs) or lack of planning could result in eventual loss of ability to mitigate the event.

(6) *Improperly communicate or coordinate control room and other plant area efforts.*
These types of failures could result in plant equipment alignments being made without full knowledge of the crew, potentially causing confusion/anxiety/stress that may further complicate the response and cause loss of safety functions or vital equipment.

(7) *Improper use of personnel for the circumstances or high room temperatures*
If the event is particularly prolonged for many hours, the use of staff resources should consider the adverse environment (high temperatures) within the plant and allow for breaks, turnovers, etc. so as to not overly tire individuals. Otherwise, poor judgments and actions may result.

D.7 Step 7: Identify and Evaluate Complicating Factors and Links to Performance Shaping Factors (PSFs)

While additional complicating factors such as random failures of equipment or indicators or alarms may make the context even more error forcing, the scenario and possible unsafe acts, as already postulated, seem sufficiently challenging. Therefore, additional complicating factors will not be addressed at this time.

Also, the most relevant PSFs have already been identified through the previous steps. These include such factors as unfamiliarity with the event, including a tendency to disbelieve it, little training and procedural guidance, adverse environment, conflicting goals, time pressure at times (e.g., shutting down diesels), limited resources, and potentially high attentional and work loads. These have already been accounted for as potentially contributing to the types of errors that could be made.

D.8 Step 8: Evaluate the Potential for Recovery

Even if the scenario occurs and is a prolonged loss of the ultimate heat sink, and if the operators were to make the types of HFEs/UAs listed in section D.6.5, there is a chance that the operators will recover from their past faults and still prevent severe core or containment damage. In order to address the recovery issue, it is necessary to understand the relationship among the HFEs/UAs listed above and the possible recovery actions that may influence the scenario outcome. To do that, an event tree is constructed and shown in Figure D.10.

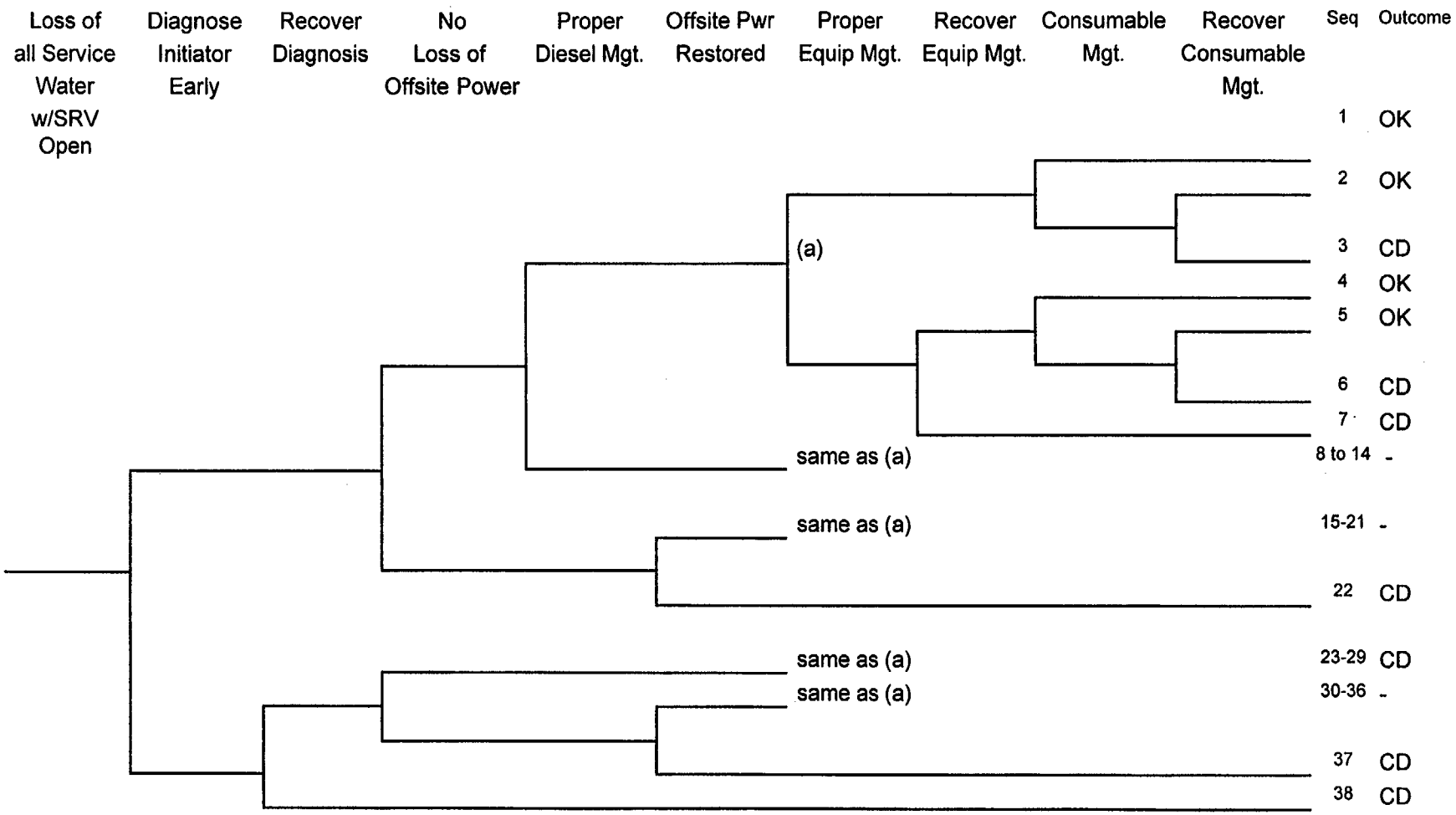


Figure D.10 Loss of Service Water Event Tree

The event tree displays the logic among the first four possible HFEs/UAs listed and their potential to lead to core damage. Also shown are the logical chances for recovering from each HFE/UA except for the diesel management failure. So little time is available to recover from a wrong decision about protecting the diesels that no chance for recovery is credited. In addition, whether offsite power is available and is recovered (if unavailable) reasonably quickly during the event can have a significant impact on the scenario outcome and so is also included in the tree structure. Note that in cases where there is a loss of normal power and it is not recovered fairly quickly, the outcome is assumed to lead to core damage (may be conservative) since it is also assumed that the diesels cannot be operated for more than a few minutes, and thus a blackout condition with loss of heat sink will soon lead to failure of the only injection system available, RCIC.

For cases where the source and extent of the initiator are not diagnosed early, it is considered that the diesels, which are apt to get a start signal, will likely not be shut down quickly enough and thus will be lost even if the extent of the initiator is eventually understood (recovered). If the initiator and its effects are not diagnosed or understood properly (the last sequence in the tree), it is assumed that the other HFEs/UAs, and therefore core damage, are likely.

The latter three HFEs/UAs listed in Section D.6.5 (numbers 5, 6, and 7) are really underlying factors that affect the likelihoods of especially HFEs/UAs, numbers 3 and 4 above. If strategy development, coordination and communication, or management of manpower resources is poor, there is a greater chance of taking the actions discussed in items 3 and 4.

The specific cues (indicator readings, alarms) and their timing related to the three recoveries in the event tree for initiator diagnosis unsafe acts, equipment management unsafe acts, or consumables management unsafe acts, cannot be explicitly delineated nor can the specific sequence of events.

This would require some additional study and thermal-hydraulic analyses not included here at this time. However, enough is known about the general nature of the cues that may induce the recovery actions that they are briefly discussed below.

Recover Initially Inadequate Diagnosis

If the operating crew has initially failed to understand the source and extent of the initiator, including its effects, many cues will become available so that the operators may correctly interpret the nature of the event and its potential ramifications. This needs to be done before damage has occurred to numerous pieces of mitigating equipment by allowing the equipment to run too long without recognition of inadequate cooling. Otherwise, there may be insufficient redundancy left to ensure maintaining the critical safety functions. As the ultimate heat sink degrades, a series of alarms and other indications will become available, which if taken together, should present a clearer means to diagnose the event. These include (for example):

- recirculation pump motor high temperature alarms
- reactor water cleanup and fuel pool heat exchanger isolations on high temperature
- CCW discharge header pressure low-low alarm
- erratic CRD pump current indications

- TBCCW header pressure indicator reads "low" or TBCCW header pressure low-low alarm
- TBCCW pump trip alarms
- TBCCW surge tank level high/low alarm
- PSW header pressure low alarm
- decreasing condenser vacuum
- auto trips of drywell and plant chillers
- SSW pump discharge pressure low alarms
- SSW pump overload and/or pump trip alarms
- HPCS SSW system trouble light lit
- various indications of trouble (erratic current, vibration, temperature, flow readings to the extent they exist) on affected equipment over time (main turbine, generator, feed pumps, ECCS pumps, room areas).

The extent of the alarms would seem to indicate that even if the initiator were to occur slowly over time so that the initial understanding of the event is not clear, the potential to understand the full nature and impact of the loss (i.e., recover the diagnosis) seems high based on the number and diversity of these indications. Hence, it is the opinion of the analysts that the likelihood of continuing to misdiagnose the event seems quite low. However, it is agreed that full understanding could come after some mitigating equipment (diesels, ECCS pumps) has been overheated or even damaged.

Recover from Poor Equipment Management

The operating crew could mis-operate mitigating equipment needed to attempt to maintain safety functions; especially if HFE/UAs numbers 5, 6, and 7 are also being made. Mis-operation could involve, for instance, letting equipment operate that is not needed or letting needed equipment operate too long and thus overheating it, or even damaging and thereby preventing its use later on. Signs of this mismanagement of the equipment will occur based on indicator readings of erratic current or flow readings where available (such cues do not exist on many pieces of equipment), low discharge pressure readings, pump trip alarms, or even signs of loss of safety functions (such as lowering RPV level). Since clear indications of overheating equipment are not often available until the equipment is already beginning to suffer degraded performance, the potential for overheating or even damaging some equipment during the scenario is judged to be high. However, the above signs of this mismanagement might make the operating crew more cautious and conservative about operating equipment as the scenario proceeds, with greater emphasis on keeping some equipment in reserve. Thus, the operating crew may become more keenly aware of needing to properly manage the use of equipment, especially if they have suffered the loss of some equipment early in the scenario. On the contrary, the demand for maintaining safety functions will be great and there will be a strong desire to operate whatever equipment is needed to do that. Hence, the extent to which the crew will learn from any initial losses of equipment due to mismanagment of equipment resources, and prevent or lessen the chances of such losses continuing to occur, is judged to be uncertain in light of this double-bind situation.

Recover from Poor Use of "Consumables"

The operating crew could mis-operate equipment in ways that quickly consume air, water, or power; especially if HFE/UAs numbers 5, 6, and 7 are also being made. Mis-operation could involve, for instance, not alternating compressor use or using compressor too often, thereby failing them; cycling SRV operation too often, using up available air and nitrogen; not dropping unnecessary electrical loads to lessen the switchgear heatup; not using portable cooling; failing to plan for water replenishment, etc. Signs of this mismanagement of the equipment will occur based on indicator readings of low air pressure, quickly falling tank levels, and room temperature alarms, among others. Since clear indications of problems may not often be discernible until the degraded conditions already exist, the potential for too quickly using up these consumables, at least at first, is judged to be high. However, as these signs do become available and with sufficient forethought about the demands on these resources, the crew could become more cautious and conservative about protecting these consumables as the scenario proceeds. On the contrary, the demand for maintaining safety functions will be great and there will be a strong desire to operate whatever equipment is needed to do that. Hence, the extent to which the crew will learn from any initial mis-managment of these consumables and prevent or lessen the chances of such mismanagement continuing to occur, is judged to be uncertain in light of this double-bind situation.

General Observations

As a whole, it can be said that cues, some direct and some indirect, will present themselves as the scenario proceeds. They will indicate the extent of the initiator and the need to better manage equipment and consumable resources. However, the cues will often be delayed and in some cases may not occur until considerable degradation of conditions has already occurred. Without a pre-thought-out plan of preferred actions, the operating crew may need to respond to events as they happen and learn (i.e., recover from previous poor judgments or actual unsafe acts) as they go, based on their observations of equipment and plant conditions that are dynamic. Hence, recovery where needed is possible; but clearly, recovering past mistakes as they happen and attempting to continue to satisfy safety function demands while avoiding equipment damage is a more difficult task without prior analyses, explicit procedural guidance, and training.

D.9 Quantification Considerations

A rough approximation is derived as to the likelihood of the event and its leading to core damage as a result of the above contributing human failures and/or unsafe acts. From Section 10, it is seen that such an assessment requires estimating the frequency of the error-forcing context (made up of the frequency of the plant condition × the probability of relevant PSFs), the probability the crew will perform the unsafe act(s), and the probability that they will not recover their original mistakes before serious plant damage occurs. Each is discussed below.

Frequency of Error-Forcing Context

The plant condition is postulated as an eventual and prolonged total failure of the ultimate heat sink, along with a stuck-open SRV during the early and numerous demands which are occurring when the balance-of-plant is isolated and subsequent pressure is controlled by the operator. The existing plant

PRA provides information to approximate this likelihood. Based on the modeled ways to lose all service water, the PRA provides an estimate of approximately 1E-5/year for the frequency of losing the ultimate heat sink for more than just a few minutes if loss of offsite power is a contributor to the event. With offsite power available, the PRA value is approximately 1E-6/year. Hence the chance of the initiator is considered to be in the E-5/year range. Considering an estimated number of SRV demands for this event (approximately a dozen or more) and the stuck-open probability per demand of about 1E-2, a likelihood of a stuck-open SRV in this event is estimated to be about 0.1 or a little greater. Combining these two values provides a frequency for the initial plant condition in the low-to-mid E-6/year range. Accounting for the need for this event to last at least in the range of 2-4 hours or more to be particularly challenging, PRA estimates for failing to recover service water or offsite power (if lost) are approximately 0.1. Hence, the likelihood of the plant condition existing for about 2-4 hours or longer is on the order of low-to-mid E-7/year.

The likelihood of the PSFs contributing to the overall frequency of the error-forcing context is considered high enough to be approximated as 1.0 since all the PSFs summarized in Section D.7 are considered by the analysts to be present and strongly influencing the performance of the operating crew given the plant condition. Hence, the estimated frequency of the error-forcing context for the postulated event is in the range of low-to-mid E-7/year.

Probability of Unsafe Act(s) and Nonrecoveries

Rather than attempting to estimate and combine the individual HFE/UA and nonrecovery probabilities, for purposes of this analysis it has been decided that a gross estimate will suffice of the crew incorrectly responding to the dynamics of the situation and performing unsafe acts that contribute to a core damage accident. Taking into account all the opportunities of the various HFEs/UAs that have been discussed and the uncertainty about the ability to recover, the analysts have worked out a consensus judgment about the likelihood of the plant staff performing unsafe acts that either directly cause or significantly contribute to core damage. This judgment is based on their experience, their understanding regarding the dynamic nature of this event, the status of procedural and training guidance, consideration of technical support staff assistance after about 1-2 hours following the trip, and factoring in the suggested values for generic tasks of a similar nature from the HEART methodology summarized in Section 10 of this report. All of these considerations collectively suggest a value of between 0.05 to about 0.5 for this estimate.

Frequency of the Event Leading to Core Damage

Combining the frequency of the error-forcing context and the probability above yields an estimate of this event progressing to core damage largely because of unsafe human interactions to be in the low E-8/year to mid E-7/year range. This is comparable to the existing core damage frequency for this initiator in the PRA of 2E-7/year.

D.10 Step 10: Issue Resolution

This analysis indicates that the likelihood of this event progressing to core damage in large part due to unsafe acts by operators is comparable to or may even be slightly greater than that already calculated in the PRA for a loss of service water initiator.

In addition, and more important, a number of lessons learned have resulted from this analysis that indicate there are improvements that could better prepare operating crews to respond properly to a prolonged loss of ultimate heat sink. The utility staff is considering the following:

- discussing with operating, maintenance, and management staff the results of this analysis and the potential contexts of concern

- performing engineering analyses and simulator runs to better understand possible sequences of events following loss of the ultimate heat sink and the identification and timing of cues indicating developing problems

- developing more explicit procedural guidance for both the operating staff and the technical support staff regarding preferred actions to be taken upon discovery of the loss of heat sink as well as ways to minimize equipment damage and use of resources during the response to such an event (where possible, utilizing guidance available in existing SBO procedures)

- developing training exercises and talk-throughs for this event that approximate various anticipated phases to the extent practicable, to familiarize the staff with its dynamics and what to expect during a prolonged loss of heat sink

APPENDIX E
ATHEANA EXAMPLE -
SMALL LOSS OF COOLANT ACCIDENT (SLOCA)
A "DIRECT INITIATOR SCENARIO"

This appendix illustrates the use of the ATHEANA process to investigate the potential for operator actions that could seriously degrade plant response to a small loss of coolant accident (SLOCA) direct initiating event. More specifically, it is an illustration of the use of ATHEANA to identify and quantify those conditions (error-forcing contexts) that may induce human unsafe acts.

This is a plant-specific example, as all fruitful examinations of context must be. However, the plant analyzed is a composite pressurized water reactor (PWR), not exactly matching any particular operating plant. The example is realistic in that all specific design, procedures, training, and operating and maintenance practice information used in the analysis have been observed in real plants. As a result, this example provides a basis for licensees desiring to investigate similar issues in their plants.

The illustration follows the steps discussed in the ATHEANA process in Section 9 of this document.

E.1 Step 1: Define and Interpret the Issue

The Emergency Operating Procedures (EOPs) applicable to SLOCA scenarios have been successfully tested in many plant simulators, with many crews. However, in a number of cases, crews have had difficulties–getting lost in inappropriate branches of the EOPS or running out of time–often because trainers running the simulations have failed large numbers of safety components and subtly related equipment.

The issue to be addressed in this application of ATHEANA is: Can reasonable variations on the SLOCA scenario be identified, such that progress through the EOPs is significantly more difficult than for the SLOCA of the Final Safety Analysis Report (FSAR) safety analysis?

It is useful to discuss the idea of "reasonable" variations, before proceeding with the analysis. The plant probabilistic risk assessment (PRA) identifies the functional failures that lead to core damage. For the SLOCA, the PRA calculates the frequency of scenarios that involve an SLOCA (frequency of SLOCA initiator) and combinations of component functional failure (probability of hardware failure and human failure to carry out expected and necessary tasks) that cause the plant functional failures that lead to core damage. From the ATHEANA point of view, there is a larger class of equipment failure, mal-alignment, and unexpected modes of operation, not currently modeled in the PRA, that, while not directly causing hardware functional failures associated with core damage, create cognitively challenging situations for the operators (error-forcing context, EFC) that can set up the operators to carry out unsafe acts (UAs) that make up human failure events (HFEs), thereby defeating functional success. The fact that a much larger set of components can affect human operator response than can directly affect hardware controlled plant functions sets up the PRA/HRA (Human Reliability Analysis) analyst to underestimate the probability of such conditions.

To the PRA/HRA analyst and, indeed, to most engineers (and even operators, if asked the question directly), the chance that additional components are failed is always lower than the chance that they are not. Such a view is supported by calculations of scenarios for which additional independent

failures are postulated. But there is something of a fallacy at work here; let's call it the fallacy of zero failures. If you pose the question to operators in a different way, you get a very different answer. If you ask an operator: when a reactor trip occurs, would you be surprised to encounter problems (i.e., failures) somewhere in the plant? The answer almost invariably will be "Not at all! There is always some valve, some controller that doesn't work just right. We just find a way around it and check it out later." Note that we are not talking about dependent, common cause failures here, but what appear to be random, independent failures. The reason that the expectation of zero additional failures is fallacious can be demonstrated by a simplified analysis.

Suppose we have several systems composed of a number of two-state components (successful or failed) with identical failure rates. Say that the failure probability of each component is "p," where p = 0.001. If the number of components in a system is "n," then the probability that k out of the n components are failed follows the usual binomial distribution:

$$P(k) = \frac{n!}{k!(n-k)!} p^k (1-p)^{n-k}$$

Now we can directly address the likelihood of zero failures (or, if a scenario has "r" failures, the chance that they are actually one, two, or more additional failures). We look at four cases where the systems have 100, 1,000, 10,000, and 100,000 components respectively (Table E.1).

Table E.1 Probability of k Failures in Systems of Various Size (p=0.001)

k	n=100	k	n=1,000	k	n=10,000	k	n=100,000
0	0.90	0	0.37	0	4×10^{-5}	0	4×10^{-44}
1	0.09	1	0.37	1	5×10^{-4}	1-64	7×10^{-5}
2	0.004	2	0.18	2	2×10^{-3}	65-74	4×10^{-3}
3-100	2×10^{-4}	3	0.06	3	8×10^{-3}	75-84	0.05
		4	0.02	4	0.02	85-94	0.23
		5	3×10^{-3}	5	0.04	95-104	0.365
		6-1000	1×10^{-3}	6	0.06	105-114	0.23
				7	0.09	115-124	0.06
				8	0.11	125-100,000	0.06
				9	0.12		
				10	0.12		
				11	0.11		
				12	0.09		

Table E.1 Probability of k Failures in Systems of Various Size (p=0.001) (Cont.)

k	n=100	k	n=1,000	k	n=10,000	k	n=100,000
				13	0.07		
				14	0.05		
				15	0.03		
				16	0.02		
				17	0.01		
				18	7×10^{-3}		
				19-33	7×10^{-3}		
				34-10,000	$< 5 \times 10^{-5}$		

We have provided more detail in the calculations than required for our purposes, but feel that the detail may be helpful for some readers. The point is that, for a system with 100 components, our intuition is quite good: the chance that there are zero failures at any randomly selected time is 90%; the chance of one failure is almost 10%; the chance of two failures is only 0.5%; and the chance of more than two failures is minuscule.

However, this situation changes quite dramatically as the number of components in the system goes up. For a plant with 1,000 components, the chances of zero or one failures are equal (37%) and the chance of two failures is about half of that (18%). There is nearly a 10% chance that three to five failures have occurred, and a very small chance that more than five are failed. If there are 10,000 components, there is almost no chance that none or only one component is failed; it is most likely that 7 to 12 are failed (64%); and there is a small chance that more than 20 have failed. Finally, if the system has 100,000 components, there is almost no chance that fewer than 65 are failed; it is most likely that 85 to 115 are failed (> 80%); and there is a small chance that more than 125 are failed.

What does this mean to a nuclear plant PRA and an ATHEANA analysis? Although actual component demand failure rates vary roughly from 1×10^{-4} to 1×10^{-2}, with a few above and below that range, the use of 1×10^{-3} in the example is not unreasonable. There are about 100 component types modeled in a typical PRA, representing about 500 to 1,000 components. So, among those components modeled in the PRA, it is likely that there are 0 to 2 failures at any particular time. As discussed above, many other components–especially instrument and control (I&C) systems, but also balance of plant components and others not modeled in the PRA–compete for the operators' attention and affect their situation assessment, workload, etc. There are typically more than 100,000 components on a plant Q-list, but not all of these have a high potential to directly affect the operators. We suspect that all told there may be 2,000 to 5,000 components among safety systems, support systems, I&C equipment (including alarms), balance of plant, and radwaste systems that

have a potential claim on the operators' attention. Therefore, while from a strictly PRA component list point of view there may be little chance that more failures exist than those identified in the PRA sequences or cut sets, from the EFC viewpoint relevant to ATHEANA, it is almost certain that several additional failures are present. Various groups of these failures form classes of EFC that may be relevant to ATHEANA analysts.

E.2 Step 2: Define the Scope of the Analysis

In this case, the scope of the initiator type is limited by the issue to SLOCA. Characteristics of the SLOCA that are challenging include the fact that inventory is being lost and, if makeup water is not supplied in short order, extensive voiding in the reactor coolant system (RCS) will occur that impedes reflood and pressure control (especially because reactor coolant pumps (RCPs) are stopped by procedure, early in the event). In addition, while there is significant heat removal via the rupture, it is not sufficient to maintain temperature or support cooldown. However, this blowdown heat removal, when combined with steam dump following turbine trip, can lead to concerns about overcooling. After a short time, no steam dump is required at all. Some time into the accident, the operators must manually switch cooling from safety injection (SI) to closed loop residual heat removal (RHR) cooling or containment sump recirculation cooling.

We anticipate that some setting of priorities among potential contextual elements may be needed to narrow the analysis to an affordable scope. Therefore, we consider additional sources of information. From a review of the events in Appendix A, we find that many serious events involve an incorrect situation assessment resulting from a combination of factors:

- a significant physical deviation in the initiator or scenario (a strongly influencing mismatch between training and plant physics in the scenario) and an instrument problem (a moderately influencing mismatch between actual conditions and indicated conditions)

- a significant bias about the initiator or scenario (a strongly influencing mismatch between training and plant physics in the scenario) and an instrument problem (a moderately influencing mismatch between actual conditions and indicated conditions, due to an instrument).

Both cases involve operators not understanding the physics of the situation combined with an instrument problem that can disrupt clear thinking about the situation.

From the examination of Appendix A and Table 9.2 in the report, we infer that physical deviations are most likely to contribute to strong EFC. Next would be crew factors such as distractions that separate the control room team, permitting a single operator to act independently. Finally, we will focus on multiple, conflicting priorities.

E.3 Step 3: Describe the Base Case Scenario

The ideal base case, as described in Step 3 of the process description in Section 9 and illustrated in the first row of Table E.2, corresponds with a consensus operator model (COM) of the event; i.e., a mental model of the event that operators have developed through training and experience, and that is consistently understood among most operators. Furthermore, it is well defined in both an operational sense and an engineering sense (thorough neutronics and thermal-hydraulics analysis support the scenario). Finally, it is well documented and realistic. Note that Table E.2 also previews the results of the SLOCA base case development that will be presented in the following paragraphs. For the SLOCA, the base case is very near the ideal case. It will be used as the stepping off point for the deviation analysis. Because the COM is a result of required training based on the FSAR, the COM is not presented separately but is discussed during the description of the reference case and the base case.

Table E.2 Characteristics of the Base Case Scenario

Type of Base Case	Consensus Operator Model	Well-Defined Operationally	Reference Analysis		Realistic
			Well-Defined Physics	Well-Documented	
Ideal	Exists	Yes	Matches COM	Yes, Public	Yes
SLOCA Base Case	Yes; the FSAR safety analysis case is well known	Yes. Annual training scenario	FSAR safety analysis case closely matches the COM, but the analysis ends, after stabilization, but before the long-term scenario is complete	Yes; FSAR	Reasonably realistic

E.3.1 The Reference Case SLOCA Scenario

The reference case SLOCA scenario is the plant FSAR analysis, "Loss of Reactor Coolant from Small Ruptured Pipes or from Cracks in Large Pipes which Actuates Emergency Core Cooling System," FSAR Chapter 14 Safety Analysis, Section 14.3.1 pages 14.3-2 to 14.3-7 plus associated Figures 14.3-1 to 14.3-7 and Table 14.3-1.

The FSAR SLOCA is a Condition III infrequent fault, i.e., "faults which may happen very infrequently during the life of the plant. They will be accommodated with the failure of only a small fraction of the fuel rods although sufficient fuel damage might occur to preclude resumption of the operation for a considerable outage time. The release of radioactivity will not be sufficient to interrupt or restrict public use of those areas beyond the exclusion radius. A Condition III fault will

not, by itself...result in a consequential loss of function of the Reactor Coolant System or of containment barriers."

As specified by 10 CFR 50 Appendix K, "ECCS Evaluation Models," the FSAR analysis is conservative in many of its details[1], but the predicted time progression of the major plant parameters is a reasonable representation of the progression of the event. The primary impact of the conservative assumptions is to overestimate the possibility of minor core damage. A number of more realistic analyses exist,[2] but are not available in the open literature. Therefore the FSAR case has been selected to define the "reference" case for the analysis.

The FSAR analysis defines a LOCA and describes the SLOCA analysis, as follows:

> *A loss-of-coolant accident is defined as a rupture of the Reactor Coolant System piping or of any line connected to the system...Ruptures of small cross sections will cause expulsion of the coolant at a rate which can be accommodated by the charging pumps which would maintain an operational water level in the pressurizer permitting the operator to execute an orderly shutdown. The coolant which would be released to the containment contains the fission products existing in it.*
>
> *Should a larger break occur, depressurization of the Reactor Coolant System causes fluid to flow to the Reactor Coolant System from the pressurizer resulting in a pressure and level decrease in the pressurizer.[3] Reactor trip occurs when the pressurizer low-pressure trip setpoint is reached. The Safety Injection System is actuated when the appropriate setpoint is reached. The consequences of the accident are limited in two ways:*
>
> *(1) Reactor trip and borated water injection complement void formation in causing rapid reduction of nuclear power to a residual level corresponding to the delayed fission and fission product decay,*
>
> *(2) Injection of borated water ensures sufficient flooding of the core to prevent excessive clad temperature.*

---

[1]Conservatisms include break size and location, assumed loss of one train of the emergency core cooling system (ECCS), degraded SI pump head, limiting core power distributions, maximum allowable deviation (drift and error) in actuation setpoints, delay in actuation of safety injection, minimum allowable volumes, minimum heat transfer, maximum initial power, maximum fission product inventory, minimum fuel/clad temperature limits, etc.

[2]Other analyses include the backup document for the Westinghouse Emergency Response Guidelines and various proprietary WCAP thermal-hydraulic reports.

[3]If the LOCA should be in the pressurizer, flow is into the pressurizer from the RCS. If it is in the pressurizer steam space (or when the level drops below the break location), level may rise even though mass is being lost. (Steam space pressure will be lower in the pressurizer than elsewhere in the RCS.)

Before the break occurs the plant is in an equilibrium condition, i.e., the heat generated in the core is being removed via the secondary system. During blowdown, heat from decay, hot internals and the vessel continues to be transferred to the Reactor Coolant System. The heat transfer between the Reactor Coolant System and the secondary system may be in either direction depending on the relative temperatures. In the case of continued heat addition to the secondary side, system pressure increases and steam dump may occur. Makeup to the secondary side is automatically provided by the auxiliary feedwater pumps. The safety injection signal stops normal feedwater flow by closing the main feedwater line isolation valves and initiates emergency feedwater flow by starting auxiliary feedwater pumps. The secondary flow aids in the reduction of Reactor Coolant System pressure. When the RCS depressurizes to 700 psia, the accumulators begin to inject water into the reactor coolant loops. The reactor coolant pumps are assumed to be tripped at the initialization of the accident and effects of pump coastdown are included in the blowdown analyses...

The postulated small break LOCA is predominately a gravity dominated accident in which the slow draining of the RCS is accompanied by the formation of distinct mixture levels throughout the RCS. These mixture levels vary with time and are dependent upon the transient two-phase transport of mass and energy, which takes place within the RCS during the course of the accident. Consequently, the degree of accuracy with which a system model is capable of simulating the RCS's response to a small break LOCA is dependent upon the model's capability to accurately model the RCS's transient mass and energy distribution...

Results

...results of the limiting break size [are presented] in terms of highest peak clad temperature. The worst break size (small break) is a 3-inch diameter break. [The 3-inch break analysis is the most thorough of the SLOCA FSAR analyses and is selected as the SLOCA reference case for the ATHEANA analysis. Note that, in the PRA, small and medium LOCAs are considered separately, because the SI systems required to successfully respond are different. The FSAR analysis considers these both as small LOCAs and seeks the limiting case in terms of nearness to critical heat flux and possibly extensive core damage.] The depressurization transient for this break is shown in Figure [E.1, with the associated flow rate to RCS given in Figure E.2]. The extent to which the core is uncovered is shown in Figure [E.3].

During the earlier part of the small break transient, the effect of the break flow is not strong enough to overcome the flow maintained by the reactor coolant pumps through the core as they are coasting down following reactor trip. Therefore, upward flow through the core is maintained. The resultant heat transfer cools the fuel rod and clad to very near the coolant temperatures as long as the core remains covered by a two-phase mixture.

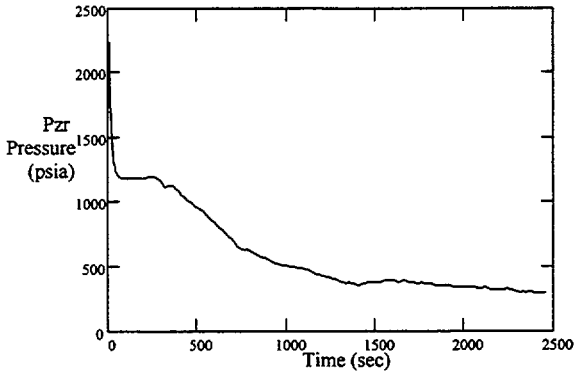


Figure E.1 RCS Depressurization Transient during 3-inch SLOCA Reference Case

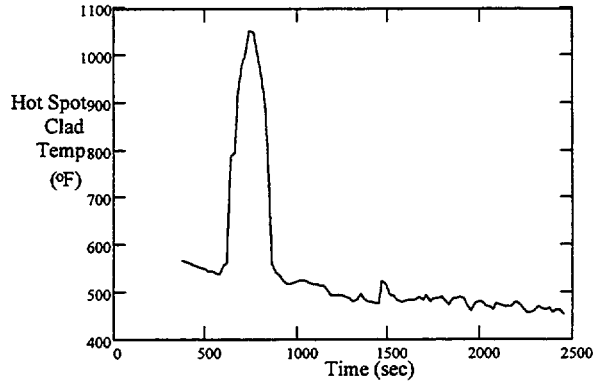


Figure E.4 Clad Temperatures Transient during 3-inch SLOCA Reference Case

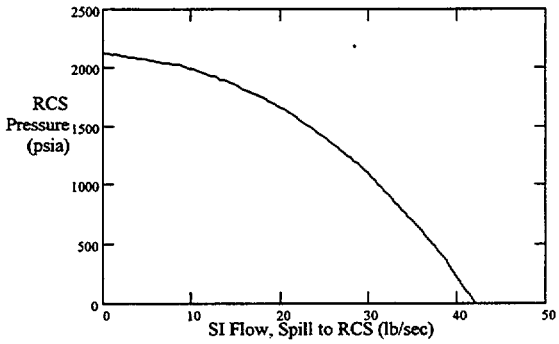


Figure E.2 Pumped Safety Injection Flow during 3-inch SLOCA Reference Case

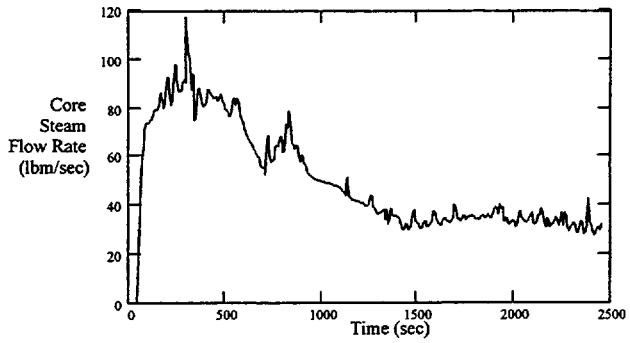


Figure E.5 Core Steam Flow during 3-inch SLOCA Reference Case

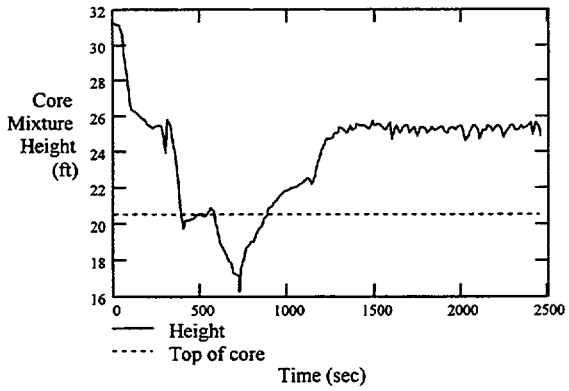


Figure E.3 Core Mixture Height during 3-inch SLOCA Reference Case

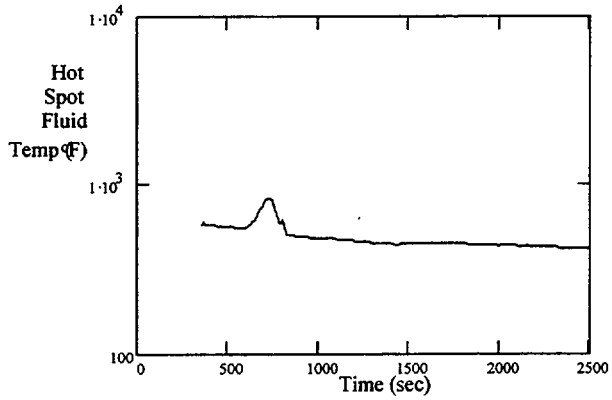


Figure E.6 Hot Spot Fluid Temperature during 3-inch SLOCA Reference Case

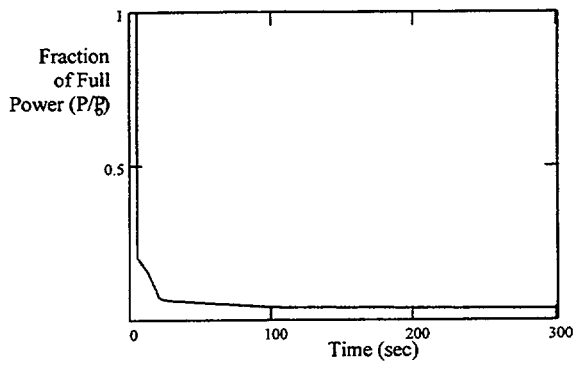


Figure E.7 Core Power during 3-inch SLOCA Reference Case

The maximum hot spot clad temperature calculated during the transient is 1020 °F including the effects of fuel densification... The peak clad temperature transients are shown in Figure [E.4] for the worst break size, i.e., the break with the highest peak clad temperature. The steam flow rate for the worst break is shown on Figure [E.5]. When the mixture level drops below the top of the core, the steam flow...provides cooling to the upper portion of the core...The hot spot fluid temperature for the worst break is shown in Figure [E.6].

The core power (dimensionless) transient following the accident...is shown in Figure [E.7]. The reactor shutdown time (5.0 sec), is equal to the reactor trip signal time (2.0 sec) plus 3.0 sec for rod insertion. During this rod insertion period, the reactor is conservatively assumed to operate at rated power.

Conclusions

...the high head portion of the Emergency Core Cooling System, together with accumulators, provide sufficient core flooding to keep the calculated peak clad temperatures below required limits of 10 CFR 50.46 [2200 °F]. Hence, adequate protection is afforded by the Emergency Core Cooling System in the event of a small break loss-of-coolant accident.

Following the TMI accident, [the vendor] performed generic studies of small break loss-of-coolant accidents. Results of these studies indicated that peak clad temperatures greater than 2200 °F may occur if the reactor coolant pumps are tripped after a significant loss of reactor coolant inventory. To prevent such a loss, the operators are instructed to trip the pumps early in the accident.

Break sizes of 2 and 4 inches were also analyzed. The depressurization transients for all three cases are shown together in Figure E.8. In all three cases, after the pressurizer empties, the pressure falls to RCS saturation pressure, about 1200 psia. As the RCS cools down, pressure again begins to fall,

faster, as expected, for larger LOCA sizes. For the 2- inch LOCA, the core is never uncovered. For the 4- inch LOCA, the core uncovers and peak clad temperature reaches 871 °F, but the effect is not as severe as for the 3-inch LOCA, where the peak clad temperature reached 1020°F.

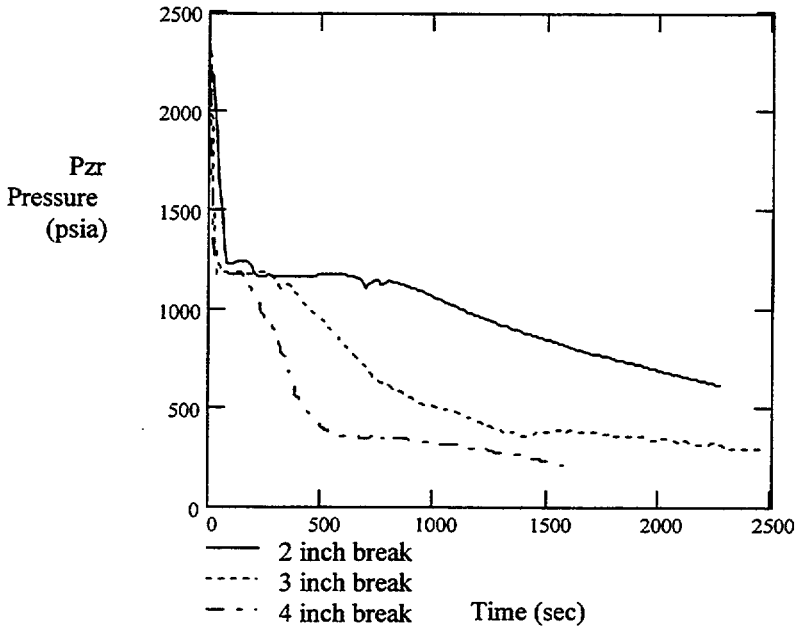


Figure E.8 Comparison of Depressurization Transients for Three SBLOCA Sizes

The key parameters observable to the operators are sketched in Figure E.9. This composite trajectory of the parameters over time constitutes a signature or pattern for the SLOCA, confirmed in reading the FSAR and training materials, and, in the simulator, where the design-basis accident (DBA) SLOCA is standard fare.

The reference scenario ends when the core is reflooded, immediate danger to the core is over, and plant parameters have stabilized, i.e., at about 40 minutes. Long-term stability is assumed as are the operator actions necessary to insure that stability.

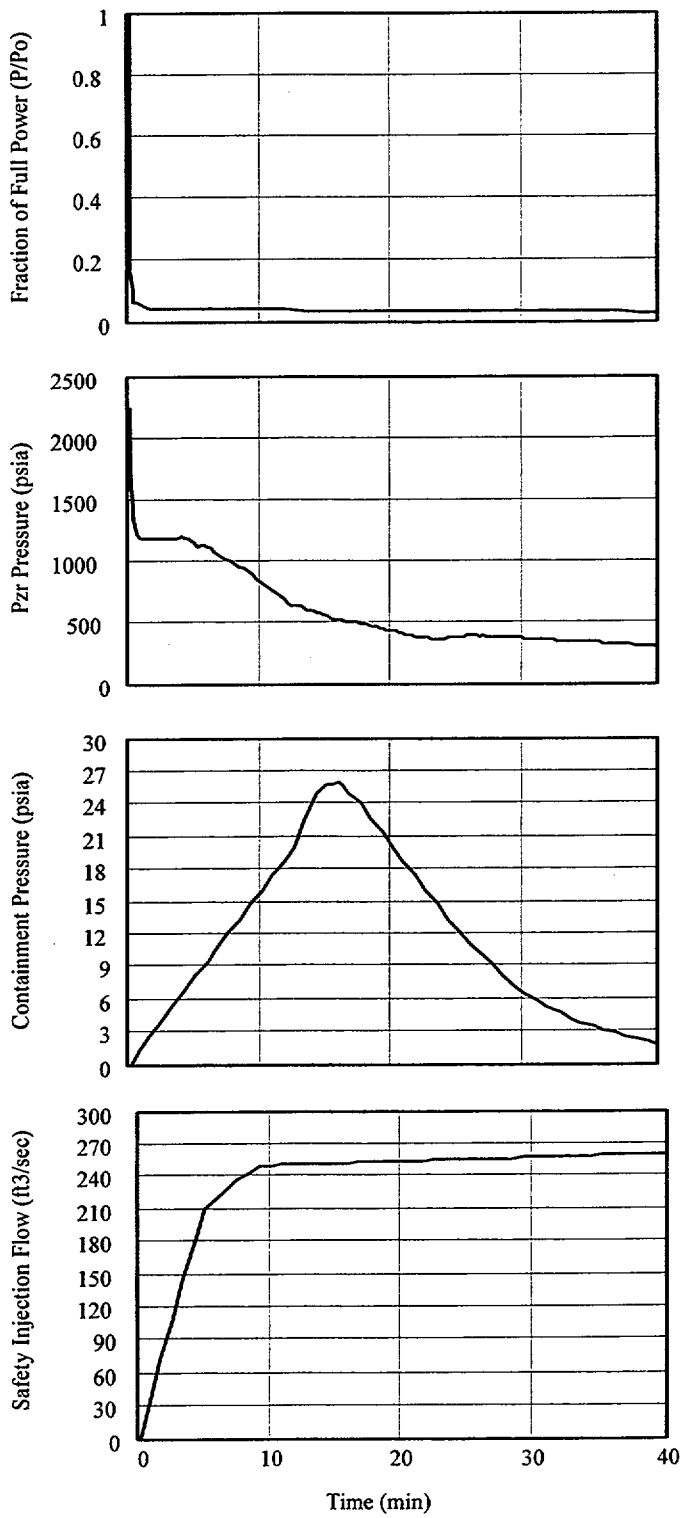


Figure E.9 Observable Parameters during SLOCA Reference Case

E.3.2 Description of the Base Case SLOCA Scenario

The base case scenario is equivalent to the reference scenario for the SLOCA over the first 40 minutes for several reasons:

- Conservatisms in the FSAR analysis of the SLOCA have only minor impact on the sequence of events and parameter changes that occur.
- The view of SLOCA held by operators is guided by their training, which includes the DBA SLOCA
  - operators undergo simulator training on the DBA SLOCA routinely, and
  - essentially all operators would define an SLOCA in terms similar to the reference case, i.e., the COM matches the reference case.

The base case scenario, however, extends well beyond the reference scenario in time. The parameters in Figures E.1 through E.8 had already stabilized. From this point on, power would continue its gradual decline, core pressure should begin to rise as the pressurizer begins to refill, ECCS flow remains about constant until pressure rises, manual switchover to recirculation cooling or RHR will be required, and peak and average clad temperature continue to decrease with falling RCS temperature.

Key points in the base case scenario not present in the reference scenario are

- Operators isolate the accumulators after switchover.[4]
- Operators align for long-term cooling, either placing the RHR system in operation or performing the switchover to recirculation cooling after the refueling water storage tank (RWST) level reaches 37% (to ensure sufficient emergency sump level to supply the RHR pump suction) and must complete the switchover before the pumps lose suction from the RWST (to prevent air binding, pump damage, and starving the core).

E.4 Step 4: Define HFEs and/or Unsafe Actions

The SLOCA event tree from the plant individual plant examination (IPE) is shown in Figure E.10. As shown in the figure, modeled systemic response to the SLOCA includes:

[4]This step is generally omitted from PRAs; thermal-hydraulic analyses in support of PRA indicate that nitrogen injection into the loops is not likely to significantly interfere with core heat removal.

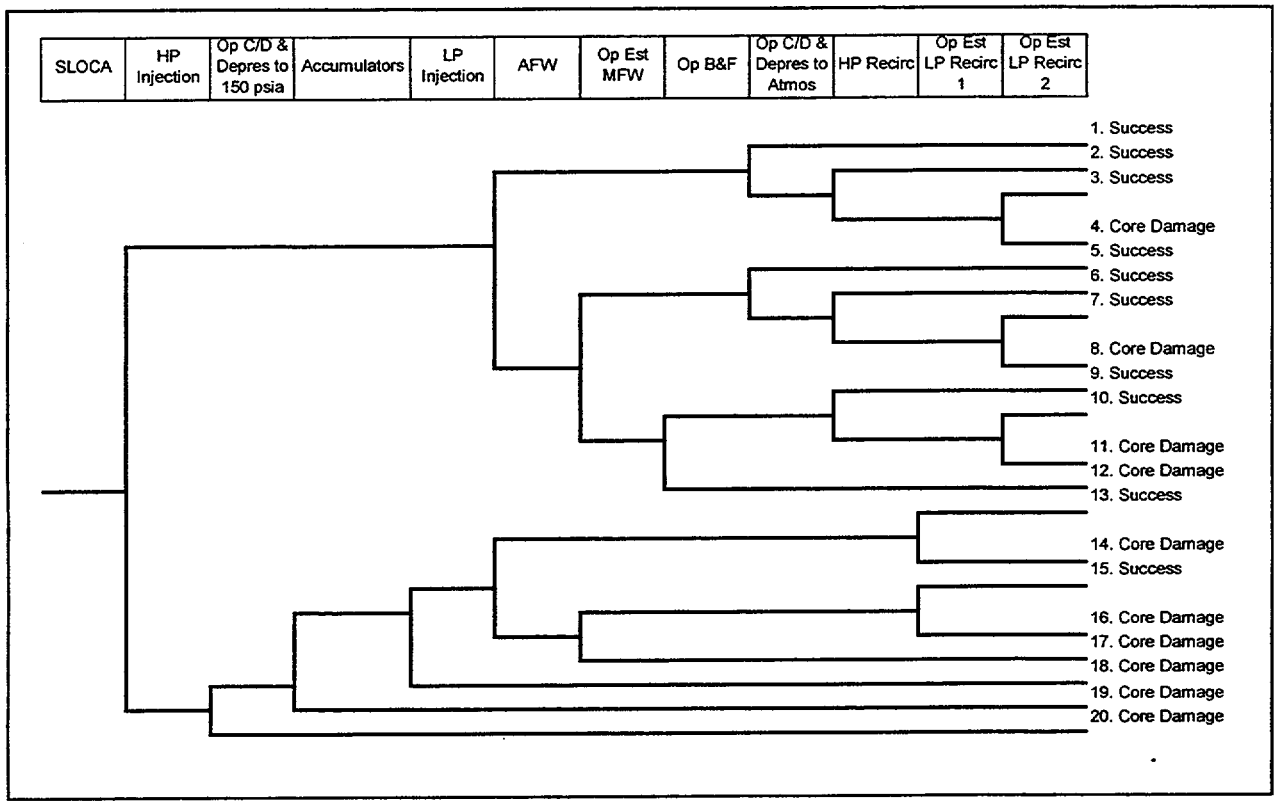


Figure E.10 Small LOCA PRA Event Tree

- high pressure injection (HPI, 1 of 2 pumps to 1 of 2 cold legs required)
- if HPI fails, operators must depressurize the RCS within 30 minutes to permit accumulator and RHR pump injection
- injection of the accumulator water (1 of 1 on the intact loop required)
- low pressure safety injection (LPI, 1 of 2 RHR pumps to the reactor vessel)
- auxiliary feedwater (AFW, 1 of 3 pumps to 1 of 2 SG)
- main feedwater (MFW), operators must align and restart (1of 2 pumps to 1 of 2 SG)
- operator establish bleed and feed (B&F) cooling within 30 minutes (open 1 of 2 pressurizer power operated relief valves (PORVs) and verify 1 of 2 SI pumps to 1 of 2 RCS cold legs)
- operator cooldown and depressurize to atomospheric pressure to minimize LOCA flow
- HP recirculation cooling (1 of 2 SI/RHR trains required)

- low pressure recirculation cooling 1 (LPR1, 1 of 2 RHR trains required); includes a required operator action to align LPR

- LPR2 is same as LPR1, except operators must depressurize via 1 steam generator (SG)

- each sequence ends in success or core damage.

Because the base case SLOCA lies just above the boundary between the small and medium LOCAs of the PRA, we examine the difference between the PRA's small and medium LOCA event trees and success criteria. First, the medium LOCA requires automatic HPI, where auto or manual is acceptable for the small LOCA. Second, if HPI fails, the medium LOCA tree requires starting operator controlled cooldown and depressurization to allow LPI in 15 minutes as opposed to 30 minutes in the small LOCA case. The last difference is that the medium LOCA case requires feedwater, only if depressurization to permit LPI is required. Similarly, B&F cooling is not required for the medium LOCA.

Finally, it should be noted that the rapid depressurization options, while potential last ditch efforts, are reached procedurally only through the critical safety function status tree for core cooling and function restoration guideline FR-C.1. This is a one-shot procedure for recovery in extremis. Likewise the MFW/condensate options are reached only through the critical safety function status tree for heat sink and FR-H.1. Thus these special actions are not reached in stepwise fashion through the procedures. If HPI fails, the EOPs instruct the operator simply to verify operation and start the pumps if they are not already running. No other recovery is directed until core exit thermocouples exceed 1200°F. This operational process is not clear from the event trees.

The ATHEANA process next asks that the systemic event tree of the plant PRA be reconstituted as a functional event tree and that other systems and human actions that can provide the same function be identified. For the SLOCA, this transformation is fairly complex because many system components and operator actions can supply each needed function as shown in Figure E.11. The functions are identified as follows:

- ***Early Makeup*** can be provided by HPI or by depressurizing—either dropping the leak rate to a point where charging pump output can match it or low enough to permit accumulator discharge followed by LPI. For pressurizer PORV LOCAs, operators can eliminate the need for makeup by closing the PORV block valves.

- ***Early Cooling*** can be provided by steaming the SGs using AFW or, if that fails, by following FR-H.1 to feed SGs with MFW, condensate, or even service water and, if all feedwater fails,

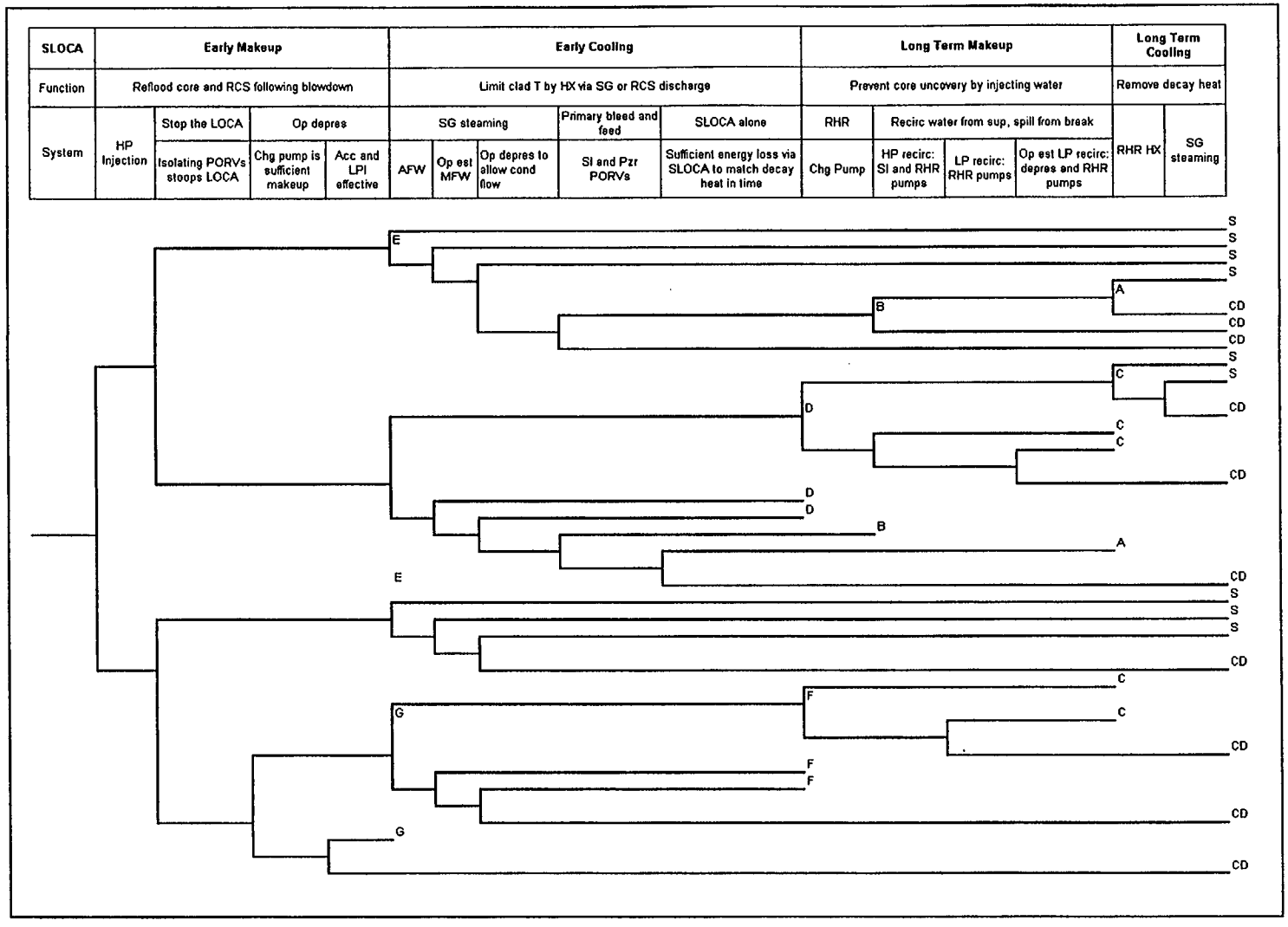


Figure E.11 Small LOCA Functional Event Tree

by aligning B&F cooling. Should B&F fail as well, it is still possible, for particular LOCAs (particular sizes and locations) and specific power time histories, that decay heat may drop to match LOCA blowdown heat removal before temperatures rise high enough to cause significant damage.

- ***Long Term Makeup*** can be provided by charging pumps if the RHR system is in service. If containment sump recirculation cooling is in operation, long-term makeup can be provided by HPR or LPR. If the plant had previously been depressurized, LPR can be placed in service directly. Otherwise, operators must depressurize the plant using an SG, before aligning LPR. Sump recirculation cooling must be initiated at an RWST level of 37% and the lineup must be completed before the RWST runs dry and the pumps are damaged.

- ***Long Term Cooling*** is generally expected to be provided by aligning component cooling water to the RHR heat exchanger for RHR or sump recirculation cooling modes. If that is not available, long-term cooling can be provided by steaming the steam generators, using hoggers, if necessary, to reach desired temperatures.

Application of the HFE identification Tables 9.6 and 9.7 of the main report would lead to a very large number of potential HFEs–several for every system level functional success criterion. Thus we need to establish priorities among all those possibilities. We first set a high priority on those issues that can lead to significant deviations in the physics of the initiating event or ensuing scenario and on those that can quickly lead to core damage. The issue of physics deviation requires a structured review that we will reserve until Step 6. However, we note at this time that failing to isolate an SLOCA associated with the pressurizer PORV can lead to conditions where steam pressures elsewhere in the RCS can be higher than in the pressurizer, which can cause the level to rise while voids are growing in the RCS. So we place a high priority on isolating the PORV. As for rapid onset of core damage, this is most likely to occur if operators interfere with HP injection or fail to align RHR or recirculation cooling before damage to the RHR pumps occurs.

Several cases appear low in priority, low enough to be screened from the analysis at this time. Later efforts in the search (i.e., identifying context that would elevate our concern) may re-introduce these issues. The first category would include errors of commission in disabling equipment that is unlikely to be needed: main feedwater, condensate, service water backup to AFW, and long-term SG cooling.

While most systems not likely to be needed can be dropped for now, until context is identified that can increase the likelihood that they will be called upon, a few will be included because their success has been important in existing PRA/HRAs. Early makeup actions to depressurize the RCS rapidly will be needed only if HP injection fails and the LOCA cannot be isolated. If the operators secure HP injection it will be because they do not believe it is needed (so they will not seek an alternative) or because they fear damage to the pumps or other equipment (in which case, they should already be planning for alternatives). The current structure of the procedures reaches this point only after the core exit temperature is very high, indicating that damage is imminent. Likewise, while it is unlikely that B&F cooling will be required, the frequency of its need has been found to be high

enough to affect risk. Therefore, failing to initiate B&F cooling is included. Note that interrupting B&F is not considered at this time, because its start requires conscious human action and we believe reversing that action will require some specific context. If a relevant context evolves out of the searches in Step 6, we can return to this issue.

The specific HFEs selected at this time include

- Operator improperly removes early makeup from armed/standby status (i.e., improper manual valve lineup blocks accumulator or RHR injection paths, control circuits blocked, or RHR pumps not in AUTO).
- Operator interrupts early makeup (i.e., operator inappropriately terminates RHR pumps).
- Operator fails to close or isolate pressurizer PORVs.
- Operator fails to depressurize RCS, when required.
- Operator fails to properly align RHR or containment sump recirculation cooling.
- Operator prematurely secures long-term makeup or cooling (RHR pumps or component cooling (CC) to the RHR heat exchangers).
- Operator inappropriately diverts resources (sump water).

All of these HFEs are within the scope of the issue defined in Step 1, if the reason for their occurrence can be attributed to a context in which the operators have difficulty applying the EOPs effectively.

E.5 Step 5: Identify Potential Vulnerabilities in the Operators' Knowledge Base

To this point, the development and description of the base case SLOCA have been based on thermal-hydraulic calculations for similar events and highlights of the most salient operator actions that are required for successful response to the scenario. A more complete operational view of the SLOCA can be obtained by examining characteristics of the scenario including information on similarities to training and experience, event timing, identification of operator tendencies, tracking of the EOPs against the scenario, and identification of informal rules that may affect operator thinking. During this process, we develop information that is helpful in identifying potential vulnerabilities that may make the HFEs more likely than they are under nominal conditions. We post this information on our blackboard for ready access during the search for deviations in Step 6.

E.5.1 Potential Vulnerabilities in Operator Expectations for the Scenario

All PRW operators receive regular training on the DBA SLOCA of the base case scenario. Therefore their expectations are very strongly aligned with the base case. Many of these simulator drills begin with a small leak that progresses to the 3-inch SLOCA. Small leaks within the capability of the charging pumps are commonplace in drill scenarios. Actual SLOCAs have occurred often enough that they are within all operators' expectations. Several of those caused operational difficulties, but it is generally believed, by operators at our plant, that only the Three Mile Island-2 (TMI-2) accident got out of hand and the causes of that event have been fixed by the current EOPs, the addition of subcooling and reactor vessel level instrumentation system (RVLIS) instruments, and changes in the training program.

On the other hand, few operators receive training on SLOCAs smaller than 3 inches (but large enough to be beyond the capability of the charging pumps) or larger than 3 inches (those greater than 2 inches are called "intermediate LOCAs" in the PRA), so deviations of this sort will be outside of their training and experience. Rules (formal and informal) may not conform with scenarios that deviate from the base case. The timing of such scenarios will be unfamiliar.

In addition, there is a strong bias that the conservatism in the DBA means that real events will be less challenging than the training scenarios. There is, it would seem, a belief that operationally challenging scenarios will align with those thermal-hydraulically challenging scenarios of the safety analysis. This belief leads to a sense that drills involving more safety system failures than in the analysis are somehow "unfair" ("You can't take away more than one SI pump!"), as if nature must play by the single failure rules of our analyses.

While there is familiarity with the base case SLOCA scenario, that familiarity breeds vulnerability to scenarios that are similar but different in timing, impact on instrumentation, and kinds and numbers of failures, and can even contribute to disbelief if scenarios involve multiple failures.

E.5.2 Time Frames for the SLOCA

From the FSAR analysis in Step 3 and the discussion of the base case scenario, five distinct time periods can be identified. These are listed in Table E.3, along with a note of the potential for operator influence.

Table E.3 Time Frames for the Base Case SLOCA

Time Frame	Occurrences	Influences on/by Operators
Initial Conditions	Steady state, 100% power No previous dependent events in base case	Routine conditions; nothing to focus attention.
Initiator/Simultaneous Events	Reactor power prompt drop Pressure drops below SI initiation point	These events are over before the operator even recognizes what is happening.
Early equipment initiation and operator response: 0-20 Seconds	Pressure drops to about 1200 psia and subcooling is lost Reactor and turbine trips ECCS flow begins MFW isolates and AFW starts Steam dump responds to turbine trip	During this time frame, the operator is checking parameters and ensuring appropriate standby equipment has started. Some early decisions in the EOPs may have occurred.
Stabilization phase 1-25 Minutes	Core reflood begins at about 10 minutes and has reached stable conditions by about 25 minutes Fuel temperatures have peaked and have fallen to match bulk RCS temperature Accumulators dump at around 10-12 minutes Pressurizer pressure has stabilized by 25 minutes and the SI pumps are delivering maximum flow Soon, as the pressurizer refills, pressure will begin to rise, SI pump flow will decrease, and subcooling will be restored	During this time, the operators have moved into the LOCA EOP and have passed a number of decision points.
Long term equipment and operator response	Isolation of the accumulators Shift to RHR or cold leg recirculation cooling Repair and recovery	Until alignment of RHR or switchover to cold leg recirculation cooling, the operators are occupied with confirmatory steps in the EOPs, depressurization, and cooldown. Any complications beyond the base case scenarios can impact their performance. This longer time frame extends to days and months. There are no critical operations concerned with the base case scenario, other than the decision to use RHR or recirculation cooling. Problems during this phase would be the concern of a low power and shutdown PRA.

By the end of the first 25 minutes, the potential for immediate damage is over; i.e., the LOCA and its direct consequences are finished, without damage to the core. All that remains is the long-term control of stable conditions. Note, however, that the operators have a number of important activities remaining, especially switchover to RHR or recirculation cooling.

E.5.3 Operator Tendencies and Informal Rules

Of the operator tendencies presented in Table 9.12a of the ATHEANA process, most factors in the SLOCA base case scenario induce appropriate tendencies to control the scenario. For example, low pressurizer level and pressure induce the appropriate tendency to increase injection. They also point toward isolating LOCA paths, decreasing letdown, and turning on pressurizer heaters.

However, after the initial blowdown, if the SLOCA is in the pressurizer, level can begin to rise, as pressurizer pressure is vented and voids form elsewhere in the RCS, possibly threatening the core. The tendency for increasing pressurizer level is to reduce injection and increase letdown–exactly the wrong response. Also later in the accident, high core heat removal (here due to the LOCA blowdown) would, in itself, encourage undesirable tendencies to decrease injection. It would also create a tendency to decrease RCS forced flow.

High containment pressure and temperature would encourage containment isolation, cooling, and spray, all useful tendencies.

A number of informal rules and practices that operators in this plant tend to observe could impact the base case SLOCA and deviations from it. A generic list of informal rules was provided in Table 9.13 of the process and, using the table to guide our thinking, we have evaluated them on a plant-specific basis. We have also evaluated plant-specific practices. The results follow:

- Protect Equipment. A recent history of running two balance of plant pumps to destruction through cavitation and overheating has made operators acutely aware of the hazards to pumps of operating with insufficient net position suction head (NPSH) and dead headed. Vibration noise is one of the factors they are most sensitive to.

- Recent History of Performance. A series of recent problems with the Channel A pressurizer pressure instrument has made operators suspicious of its performance. They tend to follow Channel B, rather than auctioneered pressure.

- Crew Characterization. Formal communications, strong shift supervisors (lower watch standers seldom question supervisor's judgments), low tolerance for perceived gaps in knowledge.

- Lack of Deep Technical Knowledge. Few shift operators have deep understanding of instrument sensor design and the algorithms used in the I&C circuits. Instrument technicians are available during day shift and can be contacted/recalled on back shifts.

Step 6 will investigate potentially negative impacts of these tendencies and informal rules in the face of deviations from the base case or other complicating factors.

E.5.4 Evaluation of Formal Rules and Emergency Operating Procedures

Perhaps the best operational view of the scenario can be developed by tracking those elements of the EOPs that are processed in the SLOCA. A "map" of these procedures is provided in Figure E.12 (provided at the end of this chapter because of its large size). The expected procedural pathway for the base case SLOCA is shown by solid arrows. The procedure map tracks all key decision points in the EOPs: (a) branch points to other procedures, (b) internal steps that disable plant functions (i.e., stopping particular plant components that can supply sometimes needed functions), and (c) steps that call out a major reconfiguration of equipment. Figure E.12 combines all procedures carried out during the base case SLOCA scenario. At each decision point (e.g., E-1, Step 2 in Figure E.12), a table in the figure provides the following information:

- Actions to be taken
- The potential for ambiguity in the decision criteria in the base case
- A judgment on the significance of taking the wrong branch or inappropriate action.

All steps that disable plant functions are indicated by hexagonal boxes (e.g., E-0, Step 20 in Figure E.12). This information is expanded to support the deviation analysis search process by indicating deviation classes under which ambiguity is increased and changes in the significance of taking wrong branches due to effects of possible deviations. For cases in which the significance could be high, the box is **bold** and the key aspects of the significance are shown in ***bold italics***. For those cases, relevant potential ambiguity is also shown in ***bold italics***. The examples cited above show these characteristics. This information will be used later in Step 6, in combination with information concerning informal rules and operator tendencies, to help insure that the consideration of deviations includes identifiable "bad actors."

The path through the procedures for the base case SLOCA is very clear and unambiguous, with the possible exception of the approach to and the decision about selecting RHR cooling or sump recirculation cooling in ES-1.2, Step 24. At this point in the accident, operators are cycling through Steps 3 to 26 of ES-1.2 Post LOCA Cooldown and Depressurization as they depressurize, cooldown, refill the pressurizer, and begin to restrict SI. There are several delicate steps in this process and one that is fairly complicated. They depressurize to allow the pressurizer to refill; depressurizing too quickly will allow voids to occur in the RCS, with resulting rapid increase in pressurizer level. Average RCS temperature (which identifies P_{sat}) must be played against pressurizer pressure to ensure subcooling to avoid erroneous level indication and passing water through the PORVs. Subcooling and pressurizer level requirements change as they proceed through these steps. Step 11, where SI pumps are stopped, has multiple requirements that depend on several plant parameters and warns that time must be allowed for pressures to stabilize after pump stops to avoid incorrect action.

If the operators are able to stabilize plant conditions including subcooling, pressurizer level, pressure <425 psig, and temperature <400°F, it is possible to place the RHR system in operation, but this

decision must be made in consultation with the Emergency Director. A lengthy discussion with plant operators and trainers indicates that this is not such an easy decision. For LOCAs near the DBA SLOCA, we are just at the point where the leak is large enough that repressurization and control are difficult and cooling is still a worry (a little larger and the heat removal through the break causes cooldown on its own). In addition, there are concerns about the viability of RHR, with regard to location of the break. If the break were in the wrong spot, aligning RHR could bypass the core. Then rising core exit thermocouples would be the only indication of the problem. The trainers, who work the technical support center during real emergencies, expressed the view that most operators would lean toward recirculation cooling because that is where the main expectations through training lie, but acknowledge that in all SLOCAs that have occurred (except the TMI-2 accident), RHR has been used. The trainers felt it would be a good exercise. Our view is that the decision point could be a source of delay and distraction, depending on the particular SLOCA.

Taking wrong branches that preclude being alert for early switchover to recirculation cooling (i.e., any path off the SLOCA path) could have serious consequences, because the time available for switchover is short and failure will lead directly to core damage.

In addition to the Figure E.12 information, the EOPs provide for continuous monitoring of "critical safety functions." CSF F-0.6 Inventory is the earliest indicator of problems and requires monitoring of the following:

- Pressurizer level (>19%)
- RVLIS (void fraction % stable or decreasing or RCP A&B OFF ≥100%).

Depending on the outcomes of these decisions, other function recovery procedures may need to be entered if additional complications occur during the scenario. These procedures ensure that operators are reminded that injection is required if pressurizer level is low. If the level is high, steps are recommended to compress voids. In particular, for SLOCA, we already noted that CSFs F-0.2 Core Cooling and F-0.3 Heat Sink are particularly important when failures of HP injection or AFW occur.

E.5.5 Summary of Potential Vulnerabilities

At the close of Step 5, we have posted on our blackboard the information collected on training and experience, time frames, operator tendencies and informal rules, and the EOP map and are ready to begin the systematic search for deviations from the base case scenario in Step 6. Before moving ahead with the search, it will be helpful to summarize the most interesting potential vulnerabilities uncovered during Step 5. That summary is presented in Table E.4.

Table E.4 Summary of Potential Vulnerabilities for SLOCA

Consideration	Observation	Vulnerability/implication
Training and experience	Annual DBA training	Expectations aligned with base case; similarity bias
	No training on SLOCAs greater than the base case	Unfamiliar, therefore weak knowledge; must adapt DBA
	Little or no training or experience on SLOCAs less than the base case, but greater than charging pump capacity	Unfamiliar, therefore weak knowledge; must adapt DBA
	Bias that DBA SLOCA is most severe and conservative case	Multiple equipment failures or ambiguities in procedures not seen in base case may strain credulity and lead to unexpected operator response
Time frames	SLOCA stabilized by 25 minutes	Intervention during this time period, while unlikely, could be serious.
	Approach to long term cooling depends on exact SLOCA; choice of RHR/recirculation may not be clear	Short time available to effect alignment/switchover.
Operator tendencies	Tendencies: most are appropriate and helpful. However, the tendency for high core heat removal and the tendency for rising pressurizer level is to decrease injection	Taken alone, overcooling or rising level implies reduced injection flow
Informal rules	Pumps will be damaged by low NPSH and deadheading	Strong tendency to stop pumps with suspected vibration noise
	History of channel A pressurizer pressure problems	Believe channel B
	Crew follows formal communications practice, with very strong shift supervisors	Low tolerance of knowledge gaps Lower level watch standers are hesitant to question shift supervisors
	Lack of deep technical knowledge of I&C, especially instrument and sensor design, and physics algorithms. No technicians on back shifts.	Operator confusion is likely if deviations from base case operations requires detailed knowledge of I&C systems

Table E.4 Summary of Potential Vulnerabilities for SLOCA (Cont.)

Consideration	Observation	Vulnerability/implication
Formal rules/EOPs	No significant ambiguities identified for the base case, except for ES-1.2, Step 24, which requires that Emergency Director decide if RHR should be placed in service. No criteria are given in the procedure for this decision. A number of steps with high potential significance were identified, which could become ambiguous depending on the deviation from the base case.	See Figure E.12 for details. Potentially significant consequences can be found at: E-0, Steps 3, 4, 6, 11, and 18-20 E-1, Steps 1, 2, 6, 12, 14, 16, and 18 ES-1.2, Steps 3, 9, 11, and 14

E.6 Step 6: Search for Deviations from the Base Case Scenario

This search is structured to identify key elements of plant conditions and some aspects of performance shaping factors that can be primary elements of EFC context for scenarios that deviate from the base case SLOCA. The resultant EFC elements will be refined in later steps of the process. Up to this point in the analysis, the process has been straightforward, proceeding in a well-defined, step-to-step progression. However, the searches described in Step 6 of Section 9, while structured, involve substantial iteration, free-wheeling exploration, and intuitive integration.

Caveat: The analyst new to ATHEANA must resist being fooled by the stepwise presentation of the search in the following paragraphs. What you are about to read is the result of many trials, dead ends, and misdirections. As described in Section 7 of the report, the ATHEANA analysis requires a broad range of multidiscliplinary knowledge: behavioral and cognitive science, the plant-specific design and PRA, understanding of plant behavior (including thermal-hydraulic performance), understanding of the plant's operational practices (including procedures, training, and administrative practices), and generic and plant-specific operating history (including incident history, backlog of corrective maintenance work orders, and current workarounds). The analysts bring this catalog of knowledge to bear, along with the blackboard full of information collected in Step 5, to find the "most significant" deviation cases. The mental process that allows this integration is complex, not well understood, and not well suited to a step-by-step description, just as the view of a chess game by an expert is more complex and effective than a brute-force look-ahead computer program. The process requires a strong facilitator/integrator, who has broad general knowledge of all the disciplines and can challenge any other experts involved in the process. Finally, even if a single analyst can bring all the requisite knowledge to the table, it is essential that others be involved to challenge assumptions, short cuts, and possibly overly narrow analysis.

E.6.1 Search for Initiator and Scenario Progression Deviations from the Base Case Scenario

This search proceeds in the manner of a hazard and operability analysis (HAZOP), by applying the series of *guide words* introduced in the process description to the base case SLOCA scenario. For

each guide word, we seek physical changes associated with the initiating event that could enable the guide word. [Scenarios can also deviate from the base case because indicators (instruments) follow the guide word, while the scenario is otherwise undisturbed, until the control systems or operators intercede, because of the deviation in instrument response. Such situations are reserved for Step 7, where other complicating factors are considered.]

Using Section 9.6.3 of the process description, the first guide word we apply is "No or Not." The idea is that the guide words trigger the imagination of the analyst to identify potentially significant scenarios. There is no concern that the guide words be independent and there should be no wasted effort worrying if a particular deviation case should be categorized under one guide word or another. The guide words are not tools for categorization, but stimulants to the imagination.

What does it mean for there to be "no" SLOCA? It could mean that the plant says it has a LOCA, when there really isn't one. In thinking this way, the plant says it has a LOCA by initiating SI (spuriously or in response to a low pressure signal) or by exhibiting low pressurizer pressure or level.

"No" SLOCA could also mean that the loss of coolant itself is less than that assumed in the DBA of the base case or that some physical parameters of the plant behave as if the SLOCA were smaller. Note that, if the SLOCA is small enough, it ceases to be an SLOCA initiator and is simply a leak, within the capabilities of the charging pumps.

"No" SLOCA Deviation Case (Spurious SI). A number of plants were plagued with spurious SIs early in their lifetimes, due to instrument problems. In plants with high head centrifugal charging pumps that start on SI, pressures can go well above normal (about 2600 psig), so overpressure and sticking open of pressurizer PORVs and safety valves would be a concern. In our plant, where normal operating pressure is well above the shutoff head of the SI pumps, the only thing that happens is that the SI and RHR pumps operate against their shutoff heads; i.e., they will soon overheat, if not turned off, and be damaged, making them unavailable if needed later. Because of plant concern for pump safety, this could become important, if combined with substantial additional challenging context.

Probably the most significant danger in the spurious SI was that operators would begin to expect it, quickly stopping SI pumps, even if they should not. The current EOPs were developed to avoid such responses, requiring that a suite of conditions be met before terminating SI. The EOPs track quite nicely for this event. Eliminating the source of the mental bias, the spurious SIs themselves, is, nonetheless, a significant measure, because strong mental bias can override procedures and training when the context becomes challenging and often when we least expect it. Given that our plant has no history of spurious SIs and that this event will not cause a pressure excursion, this event appears to have little chance to become significant and will be put aside for now.

An unnecessary SI can occur if pressure is low, but inventory has not been lost. Such events have occurred elsewhere because of stuck open pressurizer spray valves and overcooling events. The latter also lowers pressurizer level. While such events can cause confusion, they are outside the

scope of the issue defined in Step 1. They could add challenging context to reactor/turbine trip or loss of feedwater scenarios.

The spurious SI can be human induced by the actions of an instrument technician. However, we can envision no downstream dependencies associated with that activity.

"No" SLOCA Deviation Case (< 3 inches). The SLOCA can be smaller than the base case if the break size in the RCS is less than the 3-inch break assumed in the FSAR. For a 2-inch break, the depressurization transient was shown in Figure E.8. As break size decreases, the time to reach saturation at about 1200 psia is longer and the time at 1200 psia is extended. Likewise, the time until switchover to RHR or recirculation cooling is extended. The EOPs track this event quite well.

The only problems we envision for these smaller SLOCAs are that (1) focus on RHR cooling may divert attention from the RWST level (thus the low level alarm on the RWST becomes more important as a reminder that time is running out to align long-term cooling) and, conversely, (2) if expectations are strongly aligned with the base case SLOCA, there may be a failure to consider RHR cooling for long-term cooling. In the former case, failure of that alarm could jeopardize successful switchover. The latter case is not particularly significant from a safety standpoint, unless significant additional context combines with this circumstance to create delays or hesitancy, because high pressure recirculation cooling will provide long-term stability.

"No" SLOCA Deviation Case (Physical parameter behavior). The other class of "No" SLOCA scenarios that deviate from the base case SLOCA involve physical parameters of the plant behaving as if the SLOCA were smaller. Parameters identified in the reference case included

- Power. It could fail to drop on SLOCA if the core were over-moderated because of a fuel load error or a violation of control rod program management. This is certainly outside the range of training and operator mental models and could result from human unsafe acts. For now we assume that the probability of such events is low compared to other possible contributors, but it might be worth pursuing at a later date.

- Pressure. Only one phenomenological reason for delayed pressure drop has been identified. One channel of pressurizer pressure displays a processed signal, whose algorithm involves current sensed pressure, the time history of pressure for approximately the past 10 minutes, and the rate of change of pressure. Few operators are aware of this. If the SLOCA is small enough and if that channel of pressure indication is selected, then indicated pressure could lag actual pressure, giving a indication that the SLOCA is smaller than it actually is. We believe that this is such a minor and transient effect that there is no way that it will adversely affect human performance for the base case SLOCA. It is not included in summary discussion of the deviation analysis.

- Pressurizer level. As mentioned earlier, pressurizer steam space SLOCAs can behave quite differently than RCS SLOCAs, affecting level. This case is discussed in more detail below.

- Break flow. No phenomenological reason other than an actual smaller SLOCA for lower break flow has been identified and that case was discussed earlier.

- Containment pressure. The impact of passive heat sinks in the containment could significantly delay pressure rise and peak values. No important impact on operator performance has been postulated.

- ECCS flow. ECCS flow can be blocked because of pump or valve failure and these cases are modeled in the PRA. Such failures could be due to a previous HFE in which the operator improperly removed the equipment from the armed/standby status. Given the plant surveillance process, such a situation is very unlikely (although it happened at TMI).

  "Less" ECCS flow can occur, because of obstructions or impaired pump performance, or because a smaller SLOCA has occurred and pressure remains too high for full SI pump flow. The smaller (< DBA) SLOCA scenario was analyzed earlier. The actual impaired flow scenario falls naturally into two cases: those in which flow is reduced below that required to survive the initiator (this case is modeled in the PRA systems analysis) and those where it is sufficient for long-term success, but decidedly less than expected and, perhaps, less than needed to meet design criteria early on. Such cases again break into two. The first group can be immediately satisfied by depressurizing and allowing full flow by low pressures sources. Although this appears straightforward, especially in the SLOCA PRA event tree, it was pointed out in Step 4 that the procedural link to this action comes only through the critical safety function status tree for core cooling, when core exit thermocouples read greater than 1200°F. Additional context that interferes with that procedural jump would be important. In the second, flow is initially inadequate (from degraded low pressure sources or the charging pumps with decreased loss rate due to depressurization), which would delay core reflood (not observable to the operator), possible fuel damage resulting in high fission products in the RCS, and, possibly, delayed switchover to long-term cooling. Of these, the only one that is likely to be observed and of concern to the operator would be the high fission product concentration in the coolant. It is difficult to see how this would cause significant problems to the operator other than minor confusion and concern, unless this extra burden intensified the pressure due to other outside EFCs.

- Accumulator dump. Improper nitrogen pressure on the accumulators would delay or speed up their discharge, with little anticipated impact on the accident progression or, therefore, on operator response. From thermal-hydraulic analyses of LOCAs with and without accumulator discharge, impact of such problems on operator performance seems unlikely.

- Core reflood rate and timing. No phenomenological reason for delayed reflood has been identified, other than reduced ECCS flow or void formation due to a pressurizer steam space SLOCA, both described above.

- Clad temperature. No phenomenological reason for decreased clad temperature has been identified.

When we applied the other negative guide words ("Less," "Late/Never," "Too slow," "Too long," and "Part of"), we found that all lead the analysis to the same result. In this example, "No" is a surrogate for all these other words.

"No" SLOCA Deviation Case (Pressurizer steam space SLOCA). When the SLOCA occurs in the pressurizer steam space,[5] several unique processes occur. At first, the break involves only pressurizer steam or water. When pressure falls to RCS saturation pressure, the RCS fluid flows toward the pressurizer and out the break. As far as our consideration of effects on the operators is concerned, there are two primary observable manifestations of the steam space SLOCA:

- If the pressurizer vents its steam to containment more quickly than its volume is replenished by the SI system, pressurizer pressure drops below that of the saturated RCS and voids form at hot spots around the system (most likely in the core; also in the SGs, if they are not steaming). With higher pressure in the RCS, the expanding voids force water into the pressurizer and level rises quickly, even as mass is lost from the RCS.

- If the SLOCA is via the PORVs or safety valves, initial flow is into the pressurizer relief tank; i.e., the containment sees no humidity, radiation, or increasing pressure. RT pressure rises.

Figure E.13 sketches the kinds of change in parameter trajectories associated with this deviation. After initially falling, pressurizer level begins to rise, as voids form in the RCS. Pressurizer pressure will indicate slightly less than for a similar size RCS rupture (perhaps overemphasized in the sketch), because of venting in the pressurizer. If the SLOCA is via a PORV or safety valve (SV), containment pressure would be delayed until the pressurized relief tank (PRT) rupture disk (or the SV downstream rupture disk) ruptures and, if RCS pressure falls below the shutoff head of the RHR pumps, SI flow would increase dramatically.

Although operators have been sensitized to this case by the TMI-2 accident and new procedures and instruments were developed to protect against it, the scenario still offers challenges. To better understand this deviation case, we play the scenario against the EOPs, as represented in Figure E.12. We first observe that the procedures work, but we should look more closely at several steps where challenges could occur. With no additional equipment failures, the operators proceed to Step 19.a, where they check whether the pressurizer PORVs are closed; close them, if open; or isolate them by closing the block valves, if the PORVs cannot be closed. This step will end the SLOCA, if it is via a PORV, if the valve position indicators are indicating properly, and if the valves respond to closing signals. If the valves cannot be closed, the EOPs branch to E-1, Loss of Reactor or Secondary Coolant. So at this point one of five things happens:

[5] Pressurizer water space SLOCAs are included, because they will quickly become steam space SLOCAs as the blowdown progresses. SLOCAs via a PORV, a relief valve, or a break anywhere along the surge line, in the pressurizer, or in its taps will behave as a pressurizer steam space SLOCA.

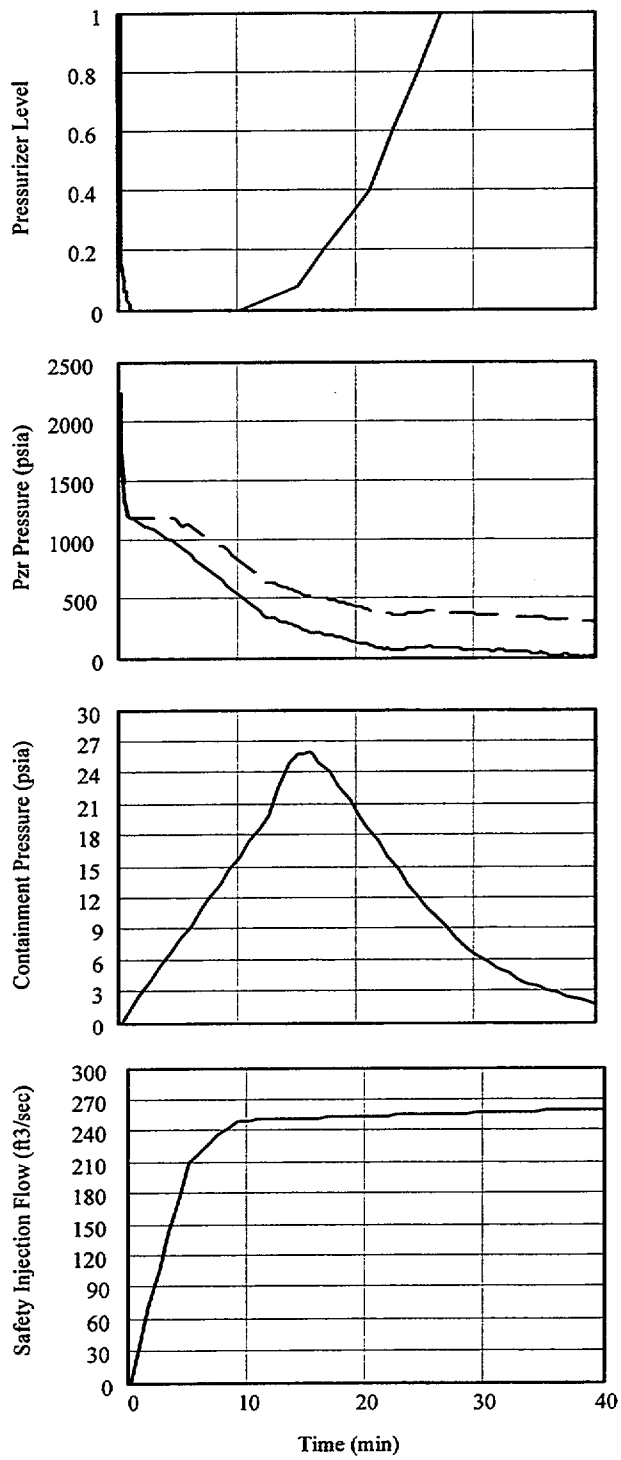


Figure E.13 Observable Parameters during Pressurizer Steam Space SLOCA Deviation Case

(1) The SLOCA is stopped. HP SI continues until the pressurizer refills and the SI pumps reach their shutoff head or until they are stopped by procedure or for some other reason.

(2) The valve position indication fails, with a PORV stuck open. This condition requires a valve failure and, perhaps, an instrumentation failure. (It may be possible for the valve to fail in a way that causes an erroneous indication.)

(3) The PORV is stuck open and the block valve fails to close. This requires two valve failures.

(4) The operators fail to properly carry out Step 19.a, continuing in the procedure with a PORV stuck open.

(5) The SLOCA is via a stuck open SV or a pipe/vessel rupture.

In the *first* case, the event is essentially over. The operators should proceed into E-1, where, at Step 12, they should transfer to ES-1.1, SI Termination. In the *second*, the operators continue believing that the PORV is shut when it is really open; i.e., they are set up for an incorrect situation assessment. In the *third* case, they know that a path from the pressurizer is open. Even though the probability of two valves failing might not be as low as one would expect,[6] this case is not particularly challenging, because the source of the SLOCA is known. Operators would branch to E-1 and later to ES-1.2, Post LOCA Cooldown and Depressurization, where SI would be reduced, the RCS depressurized, and one RCP started, which would mix any steam pockets with liquid reactor coolant, restoring pressure control to the pressurizer. At Step 24 the operators, in consultation with the Emergency Director, will decide if they should place the plant on RHR closed loop cooling, a step that can involve a difficult decision. The *fourth* case involves a lapse on the part of the operators, missing a step in the procedure and missing the open valve indication. Additional strong context would be required for this to become a significant problem. The *fifth* case is a LOCA via the SVs or a pipe/vessel break. Operationally, this looks very much like the stuck open PORV with failed position indication of the second case, in that the operators are likely to believe that the LOCA is not in the pressurizer steam space.

In all five cases, the procedures can work. The second and fifth would appear to be the most likely to cause later problems, because the operators will have formed an incorrect situation assessment. We continue this analysis of the EOP under the assumption that the PORV is open but indicating closed. The other cases will be revisited only if an additional challenging context is identified that makes them more significant.

We continue to track the second case (failed indication that PORV is stuck open) through the procedures at E-0, Step 19.b, believing that the PORV is closed. The operators are expected to have no problems due to the deviation in E-0 and should successfully transition to E-1. In E-1, all should

[6]If, by this point in the procedure, voiding in the RCS has already occurred, passing liquid through the PORVs could have further damaged them. Likewise, the block valves are not designed to close against flow, so the continuous passage of water or a steam water mixture could also lead to block valve failure.

go smoothly and at Step 18 RCS pressure will be >150 psig, so the operators should transition to ES-1.2. Because the base case did not make this transition, ES-1.2 is mapped separately in Figure E.12, which is also shown at the end of this appendix.

Continuing in ES-1.2, first note that incorrect decisions at several steps in ES-1.2 can increase the size of the LOCA, especially if RCP seal cooling has been lost. Such changes could almost double the break size and create confusion. When the SI pumps have run long enough to reestablish subcooling margin, depressurization can begin. This may be a difficult condition to reach, with no RCPs running, if large voids have formed in the RCS.

Next a warning is provided at depressurization Steps 9 and 14 that voiding can occur in the RCS that would cause rapidly increasing pressurizer (Pzr) level (the TMI scenario). In addition to the warning, the procedure progresses in stepwise fashion to limit the chance of voiding, by keeping control of the RCS level and subcooling. Nevertheless, if the context becomes sufficiently challenging, old rules can be enabled, such as the "Don't go solid" informal rule. Note that they have likely had a solid pressurizer for some time which could trigger undesired actions.

Finally, the SI pump stop criteria in Step 11.d, while familiar from SLOCA simulator drills, is fairly complex and takes time to follow correctly. It directly controls high pressure injection and therefore level, pressure and subcooling. Errors in this step can lead the operators on an unnecessary cycle through the procedure, during which time conditions can be degrading as the result of an incorrect action. Transfer to sump recirculation could be delayed because of belief that transfer to RHR cooling will occur soon. In addition to all this, the goal of ES-1.2 is to place the RCS on long-term RHR cooling or to reach a stable leak and fill condition using the charging pump for makeup. If the Emergency Director does not choose to place RHR in service in Step 24.c (e.g., because of concerns about break location) and the LOCA is greater than the capacity of the charging pump, the only procedural path to sump recirculation cooling is via the E-1 "Foldout Sheet."

One HFE identified in ATHEANA Step 4 has already occurred: Operator fails to close or isolate PORVs. Three additional HFEs could be enabled:

- Operator interrupts early makeup.
- Operator fails to depressurize RCS.
- Operator fails to properly align containment sump recirculation cooling or RHR.

The first and third HFEs are not likely without further and sufficiently challenging context. The second, failing to depressurize, could occur because of difficulties in controlling the depressurization operation, with uncollapsed steam bubbles in the RCS. Returning to the vulnerabilities summarized in Table E.4, we observe that

- The operators' bias is that the base case SLOCA is the most challenging case.

- The history of Channel A Pzr pressure problems would be unimportant without failure or erroneous indication on Channel B.

- The tendency to decrease injection with rising pressurizer level could come into play.

- If the shift supervisor takes wrong action, because of their mistaken situation assessment, the other members of the crew are unlikely to challenge that action.

- Lack of deep technical knowledge of I&C, in particular reactor vessel level indication system (RVLIS), could lead to confusion.

At this point, the possible physical deviation is well defined and has been determined to be important enough to proceed to the next part of the analysis. The results of the application of the guide word "No" to the SLOCA base case are summarized in Table E.5, which is provided at the end of the guide word analysis of this section. What remains is to look more formally at the human behavior factors affecting performance to see if the conditions presented are likely to be significantly challenging to plant operators.

The deviation scenario is examined for challenging context against the scenario descriptions and parameter characteristics listed in Tables 9-15 and 9-16. As explained in Section 9.6.3 of the process description, these tables provide a link between observable scenario/parameter characteristics and error types and error mechanisms (and information processing stages) of behavioral science. Based on the scenario analysis above and information in the tables, we find that the "No" SLOCA Deviation (Pressurizer steam space SLOCA) case involves at least five different, potentially troublesome characteristics:

- Large change in parameter; under the deviation scenario, this characteristic can affect situation assessment and response planning. In itself, this factor may have minor impact, for the drop in pressure and the initial drop in pressurizer level. These changes are well within the range observed in training scenarios. However, the large and rapid rise in level a short time later will be troublesome.

- Relative rate of change in two or more parameters is not what would have been expected; can affect situation assessment.

- Changes in two or more parameters in a short time; can affect situation assessment.

- Direction of change in parameters over time is not what would be expected; can affect situation assessment. The training our operators receive creates an expectation that steam space SLOCAs occur via the PORV and that valve indicators are accurate.

All these human complications would spell difficulty for the operator and could support the HFEs listed above. Nevertheless, the procedure can guide them through the situation successfully, if the context does not lead them to take the associated unsafe actions. For the case examined, a PORV must stick open and its position indicator must erroneously indicate closed. Additional factors, such as those identified as causing increased ambiguity in the EOP discussion above, would make the unsafe acts more likely.

"More" SLOCA Deviation Case. The next guide word to consider is "More." (The related words "Early," "Too quick," and "Too short" do not appear to be useful distinctions when applied to SLOCA.) This requires a break size greater than the 3-inch DBA SLOCA. Consider three cases:

(1) A LOCA somewhat bigger than the DBA SLOCA, but far from the DBA LLOCA
(2) An SLOCA that grows into a near-DBA LLOCA, and
(3) A very large LOCA, beyond the capability of the ECCS.

The *first* case is identical to the "No" LLOCA Deviation (<DBA) case of Appendix C (see Figure C.14). Please refer to that description of the deviation case, where the analysis argues that significant additional EFC is required to seriously challenge the operators. This case was dismissed in Appendix C, because it fell beyond the issue of physical deviations for the LLOCA. It will be considered here in our summary tables and further analysis, based on the description in Appendix C.

The *second* case is very similar to the LLOCA "Switching" Deviation case of Appendix C. The primary difference is that the physics of the situation are more likely in a normal plant, i.e., one that does not contain a flaw making temporary plugging of a LLOCA feasible. It is discussed in detail below as the "Growing" SLOCA Deviation case.

The *third* case was discussed as a deviation on the LLOCA, which is appropriate as it is even more severe than the DBA LLOCA. As described there, some of the scenarios in this group could be survived, if more than the minimum ECCS works, and that is the most likely case. These would not be generally more challenging than the base case LLOCA, as the operators would not know that the LOCA was larger than the DBA and the actions in the EOP for the DBA are equally appropriate for this case. However, should the LOCA be just beyond the capacity of the ECCS, actions to minimize the extent of core damage and reach long-term stability could be very challenging. This event is beyond the scope of the current issue, as defined for this analysis, and will not be discussed further.

"Growing" SLOCA Deviation Case. Here, as shown in Figure E.14, we begin with an SLOCA that begins to refill the pressurizer at about 20 minutes. Over the next 1.5 hours, the crew continues through E-1 and ES-1.2 to stabilize the plant–restoring subcooling margin, securing RHR pumps and SI pumps, stabilizing pressurizer level, and cooling down (reducing RCS temperature and pressure). They have the SLOCA well in hand after having a busy time of controlling conditions to permit placing RHR in service or switching to HP sump recirculation cooling. As they have depressurized, they needed to watch pressurizer level and subcooling very closely to prevent voiding in the RCS as discussed at Steps 9 and 14 of ES-1.2. Now they have a respite, with a stable plant in a well understood condition. It is at this time that the full LLOCA occurs, possibly catching the operators unawares, with no automatic way to re-establish low pressure injection.

Let us take a closer look by tracking the "Growing" SLOCA scenario through the EOPs. Again we begin with the procedure map of Figure E.12. The early plant response would carry the operators through the initial stages of E-0 with little question. If they notice the increasing pressure and limited injection flow, they might begin to suspect a steam or feed rupture inside containment. In

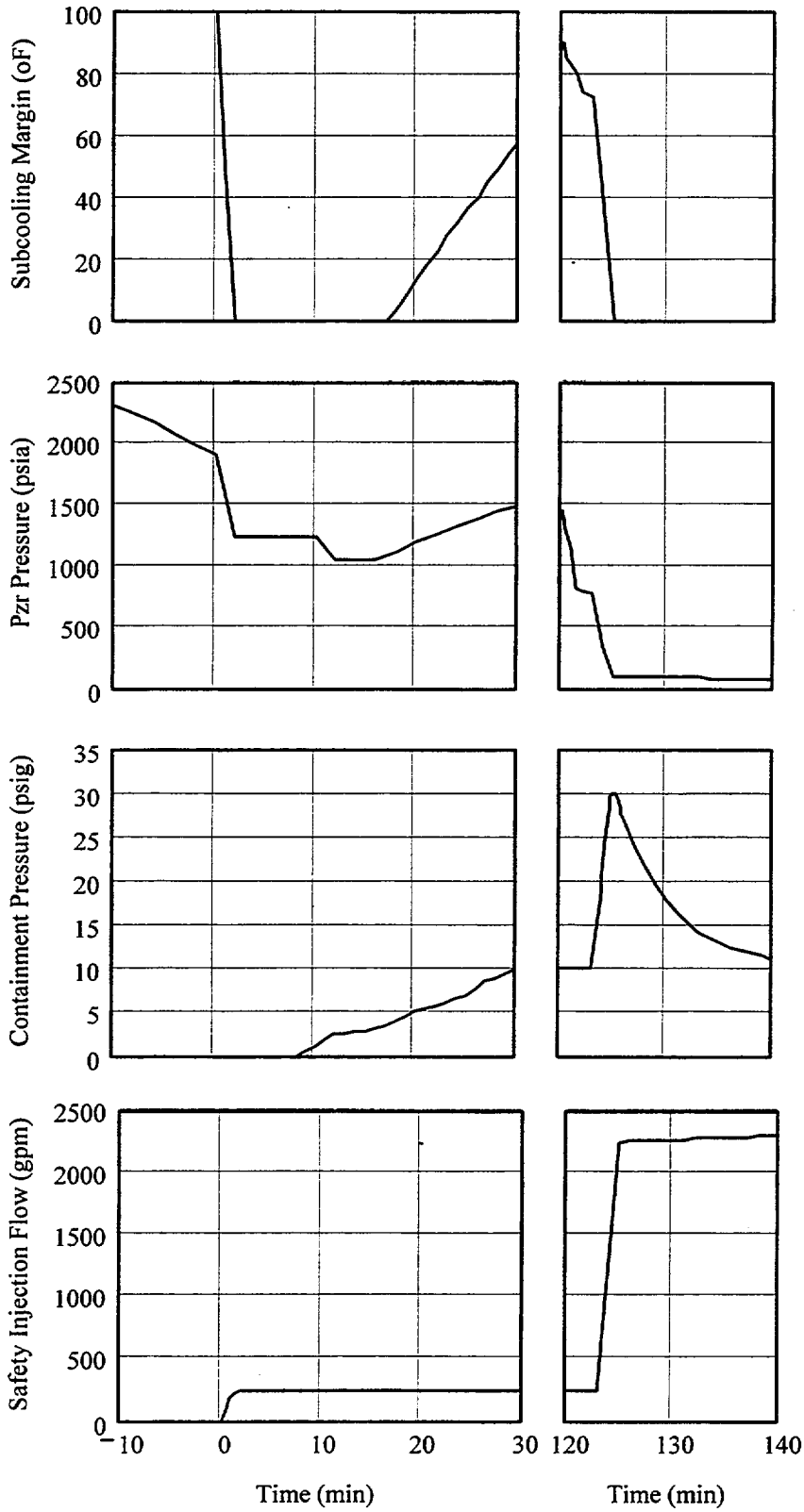


Figure E.14 "Growing" SLOCA Deviation Case

any case, faith in the diagnostic power of E-0 will still be strong. At Step 21, they should find no need to transfer to E-2, the faulted SG isolation procedure, as all SG should look the same. Even if they choose the wrong path due to a strong belief that a steam break must be the problem, E-2 will send them to E-1, loss of reactor or secondary coolant, with only a slight delay, after isolating the SGs. The loss of secondary heat sink could become a problem later, but not at this time.

In E-1, all should go smoothly initially. At Step 14, just before securing the RHR pumps (as in the base case SLOCA), the operators are cautioned that "If RCS pressure decreases in uncontrolled manner below 150 psig, RHR pumps must be manually restarted to makeup the RCS." This is an important warning for the "Growing" SLOCA scenario, but we note that there is no other caution or check for this condition other than the CSF status tree for core cooling, which looks at the core exit thermocouple readings at irregular intervals. The caution is not on the E-1 foldout sheet, which would be available as a ready reminder. When the LOCA grows sometime later, the crew will be involved in wrapping up the stable and supposedly well understood SLOCA. For now, the crew continues with E-1 until Step 18 where, because RCS pressure is above 150 psig, they should transition to procedure ES-1.2, post LOCA cooldown and depressurization. This is the same path followed by the base case SLOCA.

Continuing in ES-1.2, first note that incorrect decisions at several steps in ES-1.2 can increase the size of the LOCA, especially if RCP seal cooling has been lost. Such changes, while not a major effect, could add to confusion. The next real trap for the "Growing" SLOCA case comes in Step 3.e where, in the first cycle through Steps 3-26, the operators are again asked to stop RHR pumps, which will leave the plant with insufficient injection when the LLOCA begins. Note that this is not an error. If the pumps are not stopped, they will be damaged due to lack of flow. It is, however, an act that leaves the plant vulnerable. Failure to closely monitor pressure, while in a vulnerable state (i.e., until fully depressurized) would be a significant unsafe act.

After Step 6, they may not have recovered subcooling, so the EOP path may move on to Step 7, rather than Step 16, as shown. Next, a warning is provided at depressurization Steps 9 and 14 that voiding can occur in the RCS that would cause rapidly increasing Pzr level (the TMI scenario). In addition to the warning, the procedure progresses in stepwise fashion to limit the chance of voiding, by keeping control of the RCS level and subcooling. (The wiggles in subcooling margin and pressurizer pressure at 120 minutes in Figure E.14 are indicative of cyclic depressurization aimed at preventing voiding.) Nevertheless, if the context becomes sufficiently challenging, old rules can be enabled, such as the "Don't go solid" informal rule. Finally, the SI pump stop criteria in Step 11.d, while familiar from SLOCA simulator drills, is fairly complex and takes time to follow correctly. It directly controls high pressure injection and therefore level, pressure, and subcooling. Errors in this step can lead the operators on an unnecessary cycle through the procedure, during which time conditions can be degrading due to an incorrect action. Transfer to sump recirculation could be delayed because of belief that transfer to RHR cooling will occur soon. (Furthermore, if the LLOCA occurs during Step 11.d, the careful focus on the step-by-step rules in the EOP, especially as conditions are changing, could involve a type of "tunnel vision," delaying recognition that a LLOCA was in progress.)

The goal of ES-1.2 is to place the RCS on long-term RHR cooling or to reach a stable leak and fill condition using the charging pump for makeup. If the Emergency Director does not choose to place RHR in service in Step 24.c (e.g., because of concerns about the unknown rupture point, residual steam in the RCS binding RHR flow, or other conditions) and the LOCA is greater than the capacity of the charging pump, the only procedural path to sump recirculation cooling is via the E-1 "Foldout Sheet."

Once the LLOCA is established and, if the operators spot it in time to start the RHR pumps and save the core, it is fair to question how they would use the EOPs. They could jump back to E-0 or E-1. The case is formally included in the EOPs as cautions in E-1, Step 14, and ES-1.2, Step 3. Thus the operators could return to one of those points or carry out the action to start the RHR pumps and continue cycling through ES-1.2, Steps 3-26. The first would naturally take them to sump recirculation cooling in Step 19, if they reach that step in time. The second would simply cycle unsuccessfully hoping to refill the Pzr, when this procedure is inappropriate because the >150 psig criterion has not been met. The E-1 foldout, still in effect formally, would transfer to ES-1.3 sump recirculation.

From this discussion, it appears that, while the EOP can work for the "Growing" SLOCA deviation case, there may be some rough spots for the crew. Along the way, several actions listed as HFEs in ATHEANA Step 4 could be enabled by this deviation scenario:

- Operator removes early makeup from armed/standby status. (Note that this action to disable the RHR pumps is required by the EOP to protect the pumps and is not, therefore, an HFE. It does, however, defeat automatic response of the pumps if they are subsequently needed.)

- Operator fails to properly align containment sump recirculation cooling. (This HFE would be enabled simply by the cyclic structure of ES-1.2 and would be reinforced by the "Growing" SLOCA, because of the differences in timing introduced by a LLOCA occurring after the RWST is partially depleted by the preceding SLOCA.)

- Operator fails to manually start RHR pumps, when required. (This is a new HFE, not identified for the base case SLOCA in ATHEANA Step 4, and is introduced due to the "Growing" SLOCA deviation scenario.)

Returning to the vulnerabilities summarized in Table E.4, we observe that

- Training and experience do not directly apply; they apply to either the LLOCA or SLOCA base case, but the "Growing" deviation introduces problems in recognition, timing, and EOP ordering.

- The operator tendency to reduce injection for overcooling is very unlikely to have any impact.

- The history of Channel A Pzr pressure problems would be unimportant without failure or erroneous indication on Channel B.

- The informal rule to protect pumps from damage would reinforce the procedural stopping of RHR pumps and tend to place the focus on protecting the pumps rather than being alert to their future need.

At this point, the possible physical deviation is well defined and appears to be important enough to proceed to the next part of the analysis. It is time to look more formally at the human behavior factors affecting performance to see if the conditions presented are likely to be significantly challenging to plant operators.

The "Growing" SLOCA deviation scenario is examined for challenging context against the scenario descriptions and parameter characteristics listed in Tables 9-15 and 9-16. As explained in Section 9.6.3 of the process description, these tables provide a link between observable scenario/parameter characteristics and error types and error mechanisms (and information processing stages) of behavioral science. Based on the scenario analysis above and information in the tables, we find that this case involves at least seven different, potentially troublesome characteristics. This is not surprising; we are involved in a significant deviation from expected plant conditions outside the training and expectations of the crew. This is just the kind of situation implicated in serious accidents in which the operators are "set up" for failure. The identified scenario/parameter characteristics include

- Large (initial) change in parameter; under the deviation scenario, this characteristic can affect situation assessment and response planning. In itself, this factor may have minor impact. The change is well within the range observed in training scenarios.

- Low rate of change in parameter; can affect detection, situation assessment, and response planning.

- Changes in two or more parameters in a short time (following a period of stability); can affect detection and situation assessment.

- Garden path problem; can affect situation assessment.

- Situations that change; can affect situation assessment.

- Multiple lines of reasoning; can affect situation assessment.

These human complications spell difficulty for the operator and support the three HFEs listed above. Although the procedure can guide them through the situation successfully, there are significant factors that can defeat its success.

"More" SLOCA Deviation Case (Physical parameter behavior). The other class of "More"

SLOCA scenarios that deviate from the base case involves physical parameters of the plant that behave as if the LOCA were larger. Applying the guide word "More" to the plant parameters power, pressure, pressurizer level, containment pressure, accumulator dump, core reflood rate and timing, and clad temperature failed to yield meaningful or new scenarios, not uncovered earlier. The results for other parameters are

- Break flow. For certain SLOCA locations (e.g., near the discharge of the RCPs), a higher flow rate for the same size SLOCA could occur. Because operators have no direct indication of break size or location, such differences should have no special impact on operator performance.

- ECCS flow. Break location can impact ECCS pump flow. If the break is such that all or part of the pump flow can bypass the core, flow would be higher. This possibility is built into the success criteria. For other cases, the success criteria may be conservative. It is not observable to the operators and does not directly affect performance.

"Reversed" SLOCA Deviation Case. The next guide word is "Reversed." The notion appears to be meaningless for the SLOCA.

"As Well As" SLOCA Deviation Case. Finally, we consider "As well as," which also includes "Repeated" and "Inadvertent." No new deviation cases were uncovered when we applied these guide words to SLOCA.

Summary of Deviation Cases. Results of the preceding guide word deviation analysis are summarized in Table E.5, where, for each guide word, we summarize the identified possible physical deviations and their significance. We also indicate which of these deviation cases are considered further. The summary analysis is continued in Table E.6, where the scenario/parameter characteristics of the deviation cases from Tables 9.15 and 9.16 are presented. The analysis of these characteristics is extended in the table by identifying the associated error types and error mechanisms from Tables 9.15 and 9.16 that apply to each deviation case.

Consider the "No" SLOCA Deviation Case (Reduced ECCS Flow). If there is a major HP injection flow reduction due to obstructions, degraded pump head, or HPI pump failure, the procedural path to success has a built-in delay that restricts time available for recovery. Nevertheless, it would appear that significant additional EFC is required to delay correct operator response to the point that core damage is likely.

Next consider the "No" SLOCA Deviation Case (Pressurizer Steam Space SLOCA). The EOPs are designed to quickly stop such LOCAs. However, four cases were identified that could prevent isolation of the steam space SLOCA: LOCA not via the PORVs (via SV or pipe/vessel break); PORV stuck open, but indicates closed; PORV stuck open and block valve fails to close; and operator lapse (skip step requiring closure or isolation). The most challenging of these would be cases where the PORV indicates that it is closed, creating the impression that the LOCA is not a

Table E.5 Application of Guide Words to SLOCA Deviation Analysis

Guide Word	Possible Physical Deviation	Significance	Carry Forward? (Explained in Text)
No/Not/ Less/ Late/Never/ Too Slow/Too Long / Part of	Spurious SI	Minor. No history of spurious SI. Shutoff head of SI pumps is less than normal operating pressure, so no pressure excursion.	No
	Break size less than DBA	Unlikely to become challenging, without substantial additional context.	Not evaluated further, at this time
	Power fails to drop (fails to shutdown)	Only possible if pre-existing error violated fuel load/control requirements. Assumed very low probability.	Not evaluated further, at this time
	Reduced ECCS Flow	Reduced flow due to obstruction or impaired pump performance is either too great for success (and is therefore included in ECCS system analysis of the PRA) or impacts timing and RCS radioactivity. The latter does not appear to have significant impact on human performance. Insufficient HP injection requires rapid depressurization, outside the normal flow of the EOPs	Yes, focus on insufficient HP injection
	Pressurizer steam space SLOCA	The LOCA is ended early in E-0, provided it is via the PORV, the valve positioin indication works properly, and the valves respond to closing signals. With failed valve position indication and a stuck open PORV, or if the SLOCA is not via a PORV, incorrect situation assessment is likely.	Yes, but equipment failures required
More/ Early/ Too Quick/ Too Short	Break size greater than SLOCA DBA: Equivalent to "No" LLOCA Deviation (<DBA) Case of Appendix C	Can change timing, no longer have "right" conditions at EOP decision points. If the vulnerabilities identified in the text enable associated error mechanisms, operators could interrupt early makeup or fail to properly align sump recirculation cooling or RHR.	Yes See Appendix C for detailed analysis of this case
	Growing SLOCA: appears to stabilize as an SLOCA, later expands to near DBA LLOCA size: Similar to "Switching" LLOCA of Appendix C	SLOCA leads to disabling LPI and automatic SI actuation, operators fall into a regime where they "know" what is going on. Potentially significant impact on operations.	Yes
Reversed	None	No physical sense other than inadvertent SI, which is another identified initiating event.	No, N/A
As well as/ Repeated/ Inadvertent	No new scenarios identified	N/A	No, N/A

Table E.6 Results of SLOCA Deviation Analysis

Possible Physical Deviation	Characteristics Potentially Affecting Human Response	Potential Error Types and Mechanisms	Further Analysis and Possible Similar Scenarios
"No" SLOCA Deviation Case: Reduced ECCS Flow	Large change in parameter Situations that change (SLOCA becomes SLOCA w/o HPI) Impasse/tradeoff/double bind (cannot get to recovery action, without waiting or prematurely jumping procedures)	A number of error types and mechanisms relevant to one HFE of Step 4 (operator fails to depressurize RCS) and a new HFE (operator fails to provide continued cooling during LPI) are associated with the characteristics Error types include applying a less appropriate procedure step, missing a decision point, and failure to take needed action The underlying error mechanisms include fixation/tunnel vision, satisfying, reluctance, expectation bias, and lack of deep technical knowledge with respect to LPI cooling	Yes; additional context will be needed to have a high chance of an HFE occurring Examine the importance of continued secondary cooling following depressurization. LPI via SLOCA may not carry away sufficient heat to maintain low pressure.
"No" SLOCA Deviation Case: Pressurizer steam space SLOCA	Missing information (break location and void formation) Misleading information Multiple lines of reasoning Double bind Large change in parameter Relative rate of change in two or more parameters is not what would have been expected Higher than expected level	A number of error types and mechanisms relevant to the HFEs (operator interrupts early makeup, operator fails to depressurize RCS, and operator fails to properly align recirculation cooling or RHR) are associated with the characteristics Error types include taking inappropriate action and competing responses The underlying error mechanisms include displayed parameter matches incorrect mental template, expectation bias (primacy), over-eagerness, anxiety and tunnel vision	Yes
"More" SLOCA Deviation Case: Break size greater than SLOCA DBA [Note: the detailed writeup on this case is in Appendix C, where it was labeled "No" LLOCA Deviation Case (< DBA)]	Large change in parameter Low rate of change in parameter Relative rate of change in two or more parameters is not what would have been expected Changes in two or more parameters in a short time Direction of change in parameters over time is not what would be expected	A number of error types and mechanisms relevant to the HFEs (interrupt early makeup and fail to align recirc) are associated with the characteristics Error types include lack of attention to other parameters, failure to take account of changes in parameter, failure to attend to more relevant parameters, or failure to recognize a serious situation in time can all lead to taking inappropriate action, taking correct action too soon, and failure to take needed action The underlying error mechanisms include over-eagerness, simplifying, preoccupation, tunnel vision, and fixation	Yes, but it almost surely requires additional context (e.g., instrumentation problems or significant extraneous demands on attention) to become significant.

Table E.6 Results of SLOCA Deviation Analysis (Cont.)

Possible Physical Deviation	Characteristics Potentially Affecting Human Response	Potential Error Types and Mechanisms	Further Analysis and Possible Similar Scenarios
"More" SLOCA Deviation Case: "Growing" SLOCA: Starts as an SLOCA, later transitions to LLOCA	Large change in parameter Low rate of change in parameter, early on Changes in two or more parameters in a short time (following a period of stability) Garden path problem Situations that change Multiple lines of reasoning	A very large number of error types and mechanisms relevant to one HFE of Step 4 (fail to align recirc) and a new HFE (fail to manually initiate LPI) are associated with the characteristics Error types include lack of awareness of change, generation of false theories to explain seeming anomalies, delay in response while searching for an explanation, lack of attention to other parameters, failure to take account of changes in parameter, failure to attend to more relevant parameters, or failure to recognize a serious situation in time can all lead to missing a decision point, taking inappropriate action, and failure to take needed action The underlying error mechanisms include incredulity, over-eagerness, simplifying, preoccupation, tunnel vision, fixation, lack of deep technical knowledge, and multiple lines of reasoning are creating conflicting choices	Yes, continue. Similar scenario: LLOCA "Switching" Deviation case of Appendix C

steam space SLOCA. Despite the strong significance of this physical deviation, emphasis on meeting SI termination criteria is also strong. Some additional context is necessary for a substantial chance of the relevant HFEs.

Also consider the "More" SLOCA deviation case (> DBA). Despite the large number of error types and error mechanisms that could enable the two HFEs,

- Operator interrupts early makeup
- Operator fails to properly align containment sump recirculation cooling or RHR,

there is substantial time for the operators to respond to the many directions in the EOPs that would restore the scenario to a success path. It appears that the "No" SLOCA deviation case (> DBA) surely requires additional EFC beyond the physical deviations (e.g., instrumentation problems, hardware failures, or significant extraneous demands on attention) to become significant. Informal rules described in the text would then become important and could lead to either HFE.

Finally consider the "Growing" SLOCA deviation case. This scenario has many nearly overwhelming error mechanisms at work. On top of that, although one can track a success path through the EOPs, there are many opportunities missing and, at least for a short time, necessary pieces of information. All this is combined with unfavorable timing (very short time frame for restarting RHR pumps; a distorted picture of the time until switchover to recirculation, and, possibly, for switchover due to the long time under SLOCA conditions). In addition, there is the belief that the DBA SLOCA is the most severe SLOCA case and the disbelief that a LLOCA can actually occur. All together, this is a very strong EFC for the HFEs under consideration.

E.6.2 Search of Relevant Rules

The EOPs applying to the base case SLOCA were examined in Section 5 and yielded no strong context that would be expected to lead to error without further EFC. Four potentially challenging deviation scenarios, developed from applying the guide words to the base case SLOCA, led to a thorough review of the EOPs applied to these scenarios, under the search of Section E.6.1. In two of those cases, it was clear that additional elements of error-forcing context could change relatively benign scenarios into much more serious situations. That is the purpose of this and the following two searches is to identify additional factors that could make these scenarios more difficult for operators.

We have already walked through the EOP map of Figure E.12, identifying possible ambiguities and significance, in Steps 5 and 6.1. At this point, we can summarize those findings, in light of the identified HFEs. Generally,

- ECCS equipment is to be maintained in an armed/standby status.

- Early makeup, HPI for SLOCAs, is to be maintained until the SI termination criteria are met, at which point SI is stepped back in stages to ensure that the criteria continue to be met.

- PORVs are to be closed or isolated if an SI has occurred.
- RCS is to be depressurized if HH injection fails.
- Long-term makeup and cooling are to be maintained.

In specific cases, these functions can be terminated or unintentionally defeated:

- If indicated RWST level is less than 37%, the operators are to transfer to containment sump recirculation; doing this when actual level is higher (i.e., when level in the sump is low) could lead to vortexing and air binding the RHR system, blocking flow to the reactor.
- If pressurizer PORVs are faulty, operators are to close the block valves.
- If the SI termination criteria (subcooling >30°F and RCS pressure >2100 psig and pressurizer level >5% and secondary cooling) are met, operators are to trip SI pumps and RHR pumps.
- If RCS pressure is not falling and RHR pumps have no flow, operators are to stop RHR pumps.
- If there is no indication of high radiation in auxiliary building, the operators are not directed to search for a LOCA outside containment.
- If complex criteria are met, including pressurizer level and specific subcooling criteria depending on the number of charging pumps and RCPs running, stop SI pump(s).

Besides the above "formal" rules the informal rule/plant practice vulnerabilities identified on our Step 5 blackboard include

- Protect equipment. Operators are acutely sensitive to looking for signs of equipment degradation and rapidly shutting down affected equipment. Apparent equipment problems could lead operators to shut down needed equipment.
- Operators tend to discount Channel A pressure instruments because of the history of Channel A pressurizer pressure problems. This becomes important, in case of failure or erroneous indication on Channel B. Note that the lack of deep technical knowledge of I&C plays a role in how such a history of problems is interpreted and applied.
- The tendency to decrease injection with rising pressurizer level could come into play.

Based on the above summary, in order for any of the HFEs of concern to occur when following the formal or informal rules, one or a combination of the following must occur:

- RWST level is indicating less than 37% when really higher or the operators perceive it so
- Pressurizer PORVs indicating or appearing open, when really closed
- SI termination criteria appear to be met, when really not
- RHR pumps appear to be required (pressure appears to be falling or RHR pumps appear to be providing flow), when really not
- No observed high radiation in auxiliary building, with LOCA outside containment
- Erroneous or misinterpreted subcooling, when actually low
- Equipment trouble, real or perceived.

Each of these conditions is examined in Table E.7 against the scenario descriptions and parameter characteristics listed in Tables 9-15 and 9-16. As explained in Section 9.6.3 of the process description, these tables provide a link between observable scenario/parameter characteristics and error types and error mechanisms (and information processing stages) of behavioral science.

Based on the scenario analysis above and information in the tables, we find that the operators could be set up to carry out several of the HFEs: interrupt early makeup, fail to depressurize, fail to properly align recirculation cooling, and prematurely secure long-term makeup/cooling. Thus several of the examined contextual elements may be significant in the final scenario development. Note too that some of them require additional hardware failures and PSFs.

E.6.3 Search for Support System Dependencies

There are no valves that interface with the RCS that can be physically opened under normal RCS pressure and operating conditions, other than PORVs and safety valves (discussed elsewhere), letdown, and small sample valves. RCP seals can fail due to loss of both seal injection and component cooling. Seal LOCAs from all sources (except widespread failure of component cooling) are included in the SLOCA frequency. Widespread loss of component cooling has many significant ramifications for equipment and operators. However, it is considered as a separate initiator and is not included in the analysis of SLOCA events. It is identified here and could be the subject of a similar investigation. Likewise, loss of electric power would be considered separately.

One particular support system dependency that could be significant for our examination is that one instrument ac power bus can fail both the RWST low level alarm (not widely known among operators) and Channel B wide range pressurizer level. While the narrow range Channel A pressure instrument is the one with a history of recent problems, it is not always easy for operators to recall that the wide range pressure instrument is a separate instrument, down to the sensors. So failure or maintenance on this instrument ac bus sets up the operators on a number of counts: Channel B

Table E.7 Results of the EOP/Informal Rule Deviation Analysis

Condition	Example Causes of the Condition	Characteristics Potentially Affecting Human Response	Potential Error Manifestations	Further Analysis?
RWST level is indicating less than 37% when really higher or the operators perceive them so	Multiple level indicators in error	Missing/misleading information	Taking correct action too soon could air bind the system	Consider in final deviation scenario description (E.6.5).
	Operators mis-read indicators or anticipate levels before they are reached, especially if distracted	Attentional load/workload dividing crew attention, in light of expectation bias	Taking correct action too soon could air bind the system	No. Coordinated action by multiple crew members.
Pressurizer PORVs faulty or appear so, when really closed	Multiple PORV position indicators fail or one fails and opposite block valve fails closed.	Misleading information Attentional load/workload dividing crew attention	None immediately, but later, if operator conducting depressurization does not know PORVs blocked, there could be significant delay in depressurization Take inappropriate (incomplete) action	Consider in final deviation scenario description (E.6.5), but only if common cause failure could disable both PORV indicator and block valve or indicator.
	Previous lift of PORVs heats tailpipe or raises pressure in PRT	Misleading information causing operator to believe that PORV is open	None immediately, but later, if operator conducting depressurization does not know PORVs blocked, there could be significant delay in depressurization Take inappropriate (incomplete) action	Consider in final deviation scenario description (E.6.5).
SI termination criteria appear to be met, when not really met	Erroneous wide range pressure (reading high) would indicate high pressure, high subcooling, and erroneous RVLIS	Misleading information Garden path scenario	Take inappropriate action, i.e., operators would secure all HH injection	Consider in final deviation scenario description (E.6.5)..
RHR pumps appear to be required, when really not	Erroneous wide range pressure (reading high)	Missing/misleading information	Fail to take a needed action, i.e., operators do not stop RHR pumps, leading to overheating, failure, and unavailability, if required later	Consider in final deviation scenario description (E.6.5).

Table E.7 Results of the EOP/Informal Rule Deviation Analysis (Cont.)

Condition	Example Causes of the Condition	Characteristics Potentially Affecting Human Response	Potential Error Manifestations	Further Analysis?
	Erroneous RHR pump flow or pump current indication	Attentional load/workload dividing crew attention, in light of expectation bias	Fail to take a needed action, i.e., operators do not stop RHR pumps, leading to overheating, failure, and unavailability, if required later	Consider in final deviation scenario description (E.6.5).
	Operator misreads or misinterprets RHR pump flow or pump current indication	Attentional load/workload dividing crew attention, in light of expectation bias	Fail to take a needed action, i.e., operators do not stop RHR pumps, leading to overheating, failure, and unavailability, if required later	Consider in final deviation scenario description (E.6.5).
No observed high radiation in auxiliary building; LOCA outside containment	Failed radiation monitors	Missing information	Fail to take required action; failure to detect LOCA outside containment leads to running out of water	No. Too many redundant radiation monitors and confirmatory information (sump level), with no wide-spread common cause identified.
	Operator fails to notice alarming radiation monitors in aux bldg, with all other information	Attentional load/workload dividing crew attention, in light of expectation bias	Fail to take required action; failure to detect LOCA outside containment leads to running out of water	No. Specific requirement in EOP to check rad monitors, redundant and diverse checks. Outside scope of issue.
Erroneous or misinterpreted subcooling (similar to SI termination requirement above)	Erroneous wide range pressure (reading high) would indicate high pressure, high subcooling, and erroneous RVLIS	Misleading information Garden path scenario	Take inappropriate action, i.e., operators would secure all HH injection	Consider in final deviation scenario description (E.6.5).
	Erroneous subcooling indication	Misleading information Garden path scenario	Take inappropriate action, i.e., operators would secure HH injection pumps	Consider in final deviation scenario description (E.6.5).

Table E.7 Results of the EOP/Informal Rule Deviation Analysis (Cont.)

Condition	Example Causes of the Condition	Characteristics Potentially Affecting Human Response	Potential Error Manifestations	Further Analysis?
	Rapid progression through EOP ES-1.2, Step 11, not waiting for stabilization	Situations that change, tunnel vision Missing information, over-eagerness	Take inappropriate action, i.e., operators would secure all HH injection pumps	Consider in final deviation scenario description (E.6.5).
Equipment trouble induces shutdown by operator	Actual impending failure or damage	Must deal with situation that changes	Possible double bind between maintaining cooling and shutting down equipment	Consider in final deviation scenario description (E.6.5).
	Erroneous indication or misperception	Misleading information Over-eagerness, anxiety	Possible double bind between maintaining cooling and shutting down equipment	Consider in final deviation scenario description (E.6.5).

pressure is out of service, after the SLOCA drops pressure below the normal range; operators only have Channel A, which they do not trust; and they will receive no alarm on low RWST level, which is the normal cue to switch to recirculation cooling.

A related issue is dependency among operator actions. It is possible that, if operators identify the need for restarting RHR pumps in time, there could be some dependency between that action and the eventual action to switchover to recirculation cooling. One was identified in the discussion of the "Growing" SLOCA scenario in Section E.6.1. Depending on which procedural anchor the operators use to start the RHR pumps, they can restart E-0, jump to E-1 Step 14, jump to ES-1.2 Step 3, or simply start the pumps and continue their cycle through ES-1.2. The likelihood of being ready for recirculation, when needed, may depend on this decision.

The results of this search are summarized in Table E.8.

E.6.4 Search for Operator Tendencies and Error Types

This search could develop other potentially significant EFCs that could become contributors to core damage frequency. However, it will not be performed, because this search is a "catch-all" for deviation characteristics that might have been missed in the earlier searches, as indicated in the process description of Section 9.6.6. It is similar to the open-ended search of earlier versions of ATHEANA, albeit a more structured approach. If significant EFC/UA combinations have been identified by the earlier searches, they are more likely to be important, because they focus on elements known to be represented in serious accidents.

E.6.5 Develop Descriptions of Deviation Scenarios

Of the four deviation scenarios selected for further analysis in Table E.6, all either had sufficiently strong context that no further complicating factors were felt necessary or those complicating factors were identified in the searches of Sections E.6.2 and E.6.3:

- "No" SLOCA Deviation Case: Reduced ECCS flow requires the failure of HH injection and problems in depressurization.

- "No" SLOCA Deviation Case: Pressurizer steam space SLOCA is complete as described and has not been extended by searches in E.6.2, E.6.3, or E.6.5, because the context was deemed strong enough without further requirements that diminish the frequency of the event. Likewise, while additional complicating factors would make the context even more cognitively demanding, the scenario and possible unsafe acts, as already postulated, seem sufficiently challenging. Therefore, additional complicating factors will not be added at this time.

- "More" SLOCA Deviation Case: Break size greater than DBA SLOCA requires instrument problems to obscure the failure to reach SI termination criteria.

Table E.8 Results of System Dependency Deviation Analysis

Condition	Example Causes of the Condition	Characteristics Potentially Affecting Human Response	Potential Error Manifestations	Further Analysis?
AC instrument bus failed or out of service causing RWST low level alarm and Ch B wide range pressure to be inoperable	Hardware failure and subsequent repair activity	Garden path problem, simplifying, familiarity from drills, tunnel vision Masking, general pattern seems normal enough that operators do not detect or understand important changes (or lack of change) in some parameters Misleading information	Take inappropriate action, i.e., operators would secure HH injection pumps	Consider in final deviation scenario description (E.6.5).

"More" SLOCA Deviation Case: "Growing" SLOCA is complete and has not been extended by searches in E.6.2, E.6.3, or E.6.5, because the context was deemed strong enough without further requirements that diminish the frequency of the event. Likewise, while additional complicating factors would make the context even more cognitively demanding, the scenario and possible unsafe acts, as already postulated, seem sufficiently challenging. Therefore, additional complicating factors will not be added at this time.

It is appropriate, at this point, to summarize the key elements of these scenarios to identify those vulnerabilities, error types, and potential error mechanisms that we believe are most significant, and identify the associated PSFs. This information is presented in Table E.9.

E.7 Step 7: Identify and Evaluate Complicating Factors and Links to PSFs.

This step is addressed in Section E.6.5 above.

E.8 Step 8: Evaluate the Potential for Recovery

Recovery scenarios are different for each deviation case.

- "No" SLOCA Deviation Case: Reduced ECCS flow requires the failure of HH injection and problems in depressurization. In keeping with the issue for this analysis, we ignore the possibility that the operators anticipate high core exit temperatures and jump to function restoration guideline FR-C.1 before directed by the EOPs. Because the operators are instructed not to attempt depressurization until core exit temperatures are very high (1200°F), which should not occur until the core is substantially uncovered, there is little time for recovery if depressurization is delayed. Therefore, recovery is not considered for this case.

- "No" SLOCA Deviation Case: Pressurizer steam space SLOCA. There are few cues other than those monitored in the CSF status trees (i.e., no alarms or set points for equipment actuation). Therefore, when the CSF status trees call for action, there will be little time available and, given the entire context up to this point, the operators will face a serious dilemma; they will have all the previous indications that they are on the right track. The main hope for recovery in this case is that the technical support center engineers, in reviewing the time history of the event, will realize that steam voiding in the RCS is quite likely and direct that operators restore HH injection and proceed with depressurization and cooldown.

- "More" SLOCA Deviation Case: Break size greater than DBA SLOCA. Even if operators eventually stop HP injection, by this time the RCS has cooled significantly and would take substantial time to heat up, steam off, and begin to cause significant core damage. In addition, the technical support center would be reviewing the accident and could bring dispassionate judgment to bear on the problem. It is very unlikely that they too would not

Table E.9 Deviation Scenarios

Overall Plant Condition (Scenario)	Key Information Related to HFEs, Error Types, and Error Mechanisms	Most Relevant PSFs
"No" SLOCA Deviation Case: Reduced ECCS Flow High pressure injection fails due to pump failure. Eventually, when core exit thermocouples reach 1200F, CSF status tree sends operators to function restoration guideline that directs depressurization and LP injection	HFE of interest (fail to depressurize RCS, when required) Hardware failures: HH injection pumps Late changes in the plan–anxiety, stress, delays Despite EOPs leading to attempted depressurization coming after core is starved and has high temperature, there should be sufficient time, unless activity in delayed due to other factors Additional hardware failures. PORV and block valve position indication failed or combinations of PORV/indicator failure with failed closed block valves.	Procedure. Main EOP (E-0) not built for response to equipment failures beyond design basis, core is in extremis before alternatives to HPI are attempted Procedure/policy/practice. Inadequate crew communications allow other members of team to be unaware of action to isolate PORVs
"No" SLOCA Deviation Case: Pressurizer steam space SLOCA LOCA is via PORV with failed position indicator or via SV or pipe/vessel rupture, masking usual indication of steam space LOCA	HFEs of interest (interrupt early makeup), (fail to depressurize RCS), and (failure to properly align recirculation or RHR) Displayed parameter matches incorrect mental template [likewise, does not match incomplete mental template for steam space (PORV) SLOCA] Expectation bias Over-eagerness and tunnel vision Relative rate of change Double bind. Maintain injection and maintain pressurizer level Other distractions (likely that some additional instruments/equipment is failed)	Training/practice. Trained to believe instruments Training/practice. Belief that TMI accident is "fixed" (steam space LOCA will be via PORV and indicator cannot fail as at TMI) Training. Lack of training for off-expected accident conditions

Table E.9 Deviation Scenarios (Cont.)

Overall Plant Condition (Scenario)	Key Information Related to HFEs, Error Types, and Error Mechanisms	Most Relevant PSFs
"More" SLOCA Deviation Case: Break size greater than SLOCA DBA The SLOCA is larger, with commensurate higher blowdown flow than the 3 inch DBA SLOCA. Differences in timing can lead to unfamiliar accident progression. A failed instrument ac bus causes RWST low level alarm and Ch B wide range pressure to be inoperable	Two HFEs of interest (interrupt early makeup) and (fail to properly align recirc) The event itself does not follow the standard DBA SLOCA event of training drills As accident progresses Channel A pressure instrument hangs at some pressure, about 600 psig also causing subcooling to indicate high and RVLIS to read high The operators observe indications that would imply SI termination criteria are about to be met; while there are inconsistences (hanging pressure, hanging subcooling), these occur early on and may not be noticed, but EOPs have not yet focused attention on them. Other inconsistencies occur later; e.g., lack of pressure transient as RCPs are started. Over-eagerness, simplifying, and preoccupation allow operators to miss anomalies or fail to respond to a serious situation in time	Training/practice. Lack of training or practice for off-normal, unexpected accident conditions and problem solving Training/practice. Base case LLOCA and SLOCA used repeatedly in training HMI. Lack of trending displays allows odd parameter tracks to be put aside HMI. Lack of redundance leads to alarm failure
"More" SLOCA Deviation Case: "Growing" SLOCA Event starts as DBA SLOCA. Later, after the operators have stabilized the SLOCA and are preparing for long term cooling, the LOCA expands to near DBA LLOCA conditions.	Two HFEs of interest (fail to align recirc) and (fail to manually initiate LPI) Unexpected initial events can lead to false theories to explain seeming anomalies caused by incredulity; this allows the initial information to create early confusion and to become lost later, when it would be helpful As operators settle into the SLOCA track, they become vulnerable to the garden path problem and are susceptible to tunnel vision and fixation, simplifying the scenario by ignoring the initial LLOCA-like trends When RHR pumps are secured, the procedure warns that manual restart would be required. Nevertheless, experience and training reinforce the garden path scenario As they begin to focus on moving out of SI and into RHR cooling, they can become preoccupied with the details of EOP ES-1.2 and developing an over-eagerness to reach the stable end point All these factors permit a lack of awareness of change and of attention to other parameters Now they are set up for failure to recognize a serious situation in time; i.e., they can miss a key decision point, failing to take needed action, when RCS pressure suddenly falls because of the reinitiated LLOCA Even if they should respond in time, restarting the RHR pumps, multiple lines of reasoning about where to branch in the EOPs creates conflicting choices, delaying their attention from preparing for recirculation cooling, which will be needed very soon	Training/practice. Lack of training or practice for off-normal, unexpected accident conditions and problem solving Training/practice. Base case LLOCA and SLOCA used repeatedly in training Procedures. Insufficient warning to be prepared for rapidly increasing LOCA Lack of trending displays allows odd initial parameter tracks to be put aside

focus on inconsistent pressure and subcooling traces. Thus recovery for this case seems almost guaranteed, albeit after some very serious events have transpired. No formal recovery analysis seems to be needed.

- "More" SLOCA Deviation Case: "Growing" SLOCA. Because of the short time available for restarting RHR pump, the short time later when switchover to recirculation must begin, and the short time available to complete the switchover, recovery is not considered separately. Definition of the HFEs will include the idea that failure means failure to accomplish the activity within the time before unrecoverable damage occurs.

E.9 Step 9: Quantification Considerations

The issue to be addressed in this analysis was: Can reasonable variations on the SLOCA scenario be identified, such that progress through the EOPs is significantly more difficult than for the SLOCA of the FSAR safety analysis? This question can generally be answered without formal quantification of the HFEs. However, the idea of "reasonable variations" must include some sense of likelihood and this may require formal quantification, depending on the particular case, as defined in Table E.9, shown earlier.

We consider each of the four deviation cases separately, in the following paragraphs:

- "No" SLOCA Deviation Case: Reduced ECCS flow
- "No" SLOCA Deviation Case: Pressurizer steam space SLOCA
- "More" SLOCA Deviation Case: Break size greater than DBA SLOCA
- "More" SLOCA Deviation Case: "Growing" SLOCA

E.9.1 "No" SLOCA Deviation Case: Reduced ECCS Flow

No quantification will be performed. The scenario is interesting in that the normally modeled response to failure of HH injection is more difficult than usually acknowledged. However, the only combinations of failures that we have postulated to cause delay in depressurization are very low in frequency and not especially likely to cause significant delay. The fact, noted in Step 1, that some instrument/equipment failures that may attract the operators' attention are sure to have happened, does not seem sufficient in itself. There is some time for the operators to deal with those events, before the trigger point for depressurization is reached. Other unconnected failures placing high demands on the operators are unlikely, so the frequency of such scenarios would be rather low.

While this may not be a "reasonable" contributor to core damage, the initial deviation, failure of HH injection, is a reasonable variation in the SLOCA scenario and is modeled in all PRAs. Therefore, it will be addressed in the issue resolution section below.

E.9.2 "No" SLOCA Deviation Case: Pressurizer Steam Space SLOCA

Although this case appears to be a challenging deviation, on its face, because of its similarity to the "fixed" TMI-2 scenario, its "reasonableness" and degree of significance is likely to be questioned. Therefore, a more complete quantification is prudent.

Frequency of Error-Forcing Context. The full deviation case outlined in Table E.9 involves either an SLOCA via a stuck open PORV with failed position indication (indicating closed) or an SLOCA via a stuck open SVs or pressurizer pipe/vessel rupture. From the PRA we estimate the frequencies of these cases as follows:

Freq = F(stuck open PORV and failed VPI) + F (stuck open SV) + F (rupture)

If the PORV disk separates from the stem and lodges where it does not block flow, then the valve will indicate closed but be passing fluid. This was not the failure mode envisioned when the TMI fixes were made. Although the failure mode is much less likely (about $1x10^{-6}$ to $1x10^{-7}$ per year) than a simple stuck open PORV ($1x10^{-3}$ per year), it is more likely than the coincident failure of the PORV and its indication system. The pipe/vessel rupture frequency for the entire RCS is $5x10^{-3}$ per year in the PRA data and if the pressurizer and surge line are one tenth of that, the frequency is $5x10^{-4}$ per year. Finally, the frequency of open safety valve initiators is $5x10^{-3}$ per year, but this is based on minor events of reactor trip associated with an open relief or safety valve (with some limited blowdown and closure before SI). A rough estimate of the chance of an SLOCA may be based on combining this frequency with a generic probability of sticking open an SV of $5x10^{-3}$ per demand or a total frequency of $3x10^{-5}$ per year. So the frequency of the scenario is on the order of $5.3x10^{-4}$ per year.

Probability of Unsafe Acts. We address the probability of the UAs including non-recovery in an integrated one-step process. Thus we evaluate

$P(UA_1)$ = P(operators interrupt early makeup),

$P(UA_2)$ = P(operators fail to depressurize RCS | do interrupt early makeup), and

$P(UA_3)$ = P(they fail to complete the sump recirculation cooling lineup before the RWST runs dry | they do not perform UA_1 or UA_2).

Taking into account the deviation scenario, including the associated EFC documented in Table E.9 and the time available for each action, the analysts have developed a consensus judgment of the likelihood of the crew performing these UAs. Their judgment is based on their experience, their observations of many crews in the plant and in simulators, and their understanding of the context of this event, including the status of procedures and training discussed earlier. Given the difficult context of the scenario, our estimates are

$P(UA_1) =$	0.10;	i.e., perhaps 1 in 10 crews would be set up sufficiently to carry out UA_1.
$P(UA_2) =$	nearly 0;	i.e., if they interrupt early makeup, it is because they believe that the core is protected, so there is no need to carry out this act.
$P(UA_3) =$	0.01;	i.e., about 1 crew in 100 would be likely to miss the time window available for transfer to recirculation cooling, given the context.[7]

Our estimate for UA_1 is reasonably consistent with the generic estimates in HEART.

Frequency of the Event Leading to Core Damage. Combining the frequency of the EFC and the probability of the HFEs yields an estimate of core damage frequency of about $5x10^{-5}$ per year for the operators in the control room. When the technical support center team is factored into the analysis, our team believes that there is roughly 1 chance in 100 that they will miss the voiding and allow the operators to continue on their chosen path. Thus we believe that the core damage associated with this scenario is very low, perhaps on the order of $5x10^{-7}$ per year, when the technical support center is included.

E.9.3 "More" SLOCA Deviation Case: Break Size Greater then DBA SLOCA.

In this case, the scenario becomes very difficult, because of the misleading readings and lack of encouragement to question unfamiliar and confusing conditions. We think that this scenario meets the issue on its face and without complete quantification.[8] We note that previous detailed

---

[7]As a sanity check on these estimates, we examine the suggested values for generic tasks of a similar nature from the HEART methodology summarized in Section 10. First we must match our actions and EFC with those in HEART. The following are reasonable matches:

- Stopping the HH injection pumps is, in the words of HEART, a "routine, highly practiced, rapid task involving relatively low levels of skill" (0.007 - 0.045), but EFC is "unfamiliarity with a situation that is potentially important, but which occurs infrequently or is novel" (multiplier of up to 17 and we would judge it to be in about the upper third of the range). The associated probability is roughly 11 * 0.02 or 0.22, with uncertainty of 0.08 to no more than 0.5.
- Switchover to recirculation cooling is, in the words of HEART, almost a "complex task requiring a high level of comprehension or skill" (0.12 - 0.28). It is tempered by the fact that they did continue with SI despite the strength of the EFC. The associated probability from HEART is 0.16 and ranges from 0.12 to 0.28. This is substantially higher than our estimate.

[8]The interested reader will find that a very similar scenario was identified through a less direct process, in a trial of an earlier version of ATHEANA (NUREG-1624). That analysis proceeded by identifying potential HFEs; searching procedures and informal rules for rules that would direct the HFE, if used improperly; and then trying to add on plant and human context that would enable the HFE. There was no direct search for deviations or procedure mapping, so success depended on close familiarity with EOPs by operators on the analysis team and a rather free association of principles from behavioral science with plant conditions and the HFE, to complete the context. The scenario of the previous analysis included an initiating event that is nearly identical to the "No" LOCA deviation case; that analysis also identified significant failures in instruments. The conditional probability of the HFE and failure to recover was quite high (0.8 and 0.1). However, the plant-specific probability of the particular postulated instrument failure was very low, leading to a very small contribution to core damage frequency.

quantification of a similar case found a high probability of committing the UA.

E.9.4 "More" SLOCA Deviation Case: "Growing" SLOCA

Quantification of the "Growing" SLOCA deviation case is appropriate, because the resulting LLOCA is a DBA and may not be expected to present any difficulties. After all, the DBA is shown to avoid undue consequences in the FSAR and the EOPS have been well tested against this event. Quantification will focus first on the probability of the UAs, given the scenario.

Probability of Unsafe Acts. We address the probability of the UAs including non-recovery in an integrated one-step process. Thus we evaluate

$P(UA_1) =$ P(operators fail to restart RHR pumps | EFC), and

$P(UA_2) =$ P(they fail to complete the sump recirculation cooling lineup before the RWST runs dry | they restart RHR pumps $\wedge$ EFC).

Taking into account the deviation scenario, including the associated EFC documented in Table E.9 and the short time available for each action, the analysts have developed a consensus judgment of the likelihood of the crew performing these UAs. Their judgment is based on their experience, their observations of many crews in the plant and in simulators, and their understanding of the context of this event, including the status of procedures and training discussed earlier. Given the difficult context of the scenario our estimates are

$P(UA_1) =$ 0.30; i.e., they are only slightly more likely to restart the pumps than not.

$P(UA_2) =$ 0.07; i.e., about 1 in 15 crews would be trapped by the short time, multiple lines of reasoning, and deceptive timing, and fail to shift to recirculation in time.[9]

---

[9]As a sanity check on these estimates, we examine the suggested values for generic tasks of a similar nature from the HEART methodology summarized in Section 10. First we must match our actions and EFC with those in HEART. The following are reasonable matches:

- Restarting the RHR pumps is in the words of HEART, a "routine, highly practiced, rapid task involving relatively low levels of skill," but EFC is "unfamiliarity with a situation that is potentially important, but which occurs infrequently or is novel." The associated probability is no more than 17 * 0.02 or 0.34, with uncertainty of 0.12 to no more than 0.77.
- Switchover to recirculation cooling is in the words of HEART, almost a "complex task requiring a high level of comprehension or skill." It is tempered by the fact that they did restart the pumps and hardened by the strength of the EFC. If we assume that the positive impact of having restarted the pumps balances the difficult EFC, the associated probability from HEART is 0.16 and ranges from 0.12 to 0.28.

Our estimate for UA_1 is surprisingly consistent with the generic estimates in HEART. Our estimate for UA_2 is lower than HEART by about a factor of 2; i.e., reasonably close.

Frequency of Error-Forcing Context. To be consistent with the PRA, we note that their estimate of the frequency of LLOCA is 1×10^{-4} per year.[10] The frequency of SLOCA is much higher, but we have no good way to move from the SLOCA to the LLOCA. Starting with the LLOCA frequency, we ask, is it reasonable that a LLOCA would begin full bloomed? Or is it more likely that it would begin small, and grow larger after some time at lower blowdown rates? First, we observe that the few ruptures that have occurred in our direct experience began as very small leaks, and later expanded, although never to the size we are discussing. The forces due to vibration, rapidly changing temperature, or other causes seems to lead to progressive failure. We estimate that one in ten LLOCAs could begin quite small (SLOCA size or somewhat larger) and later expand significantly. So the frequency of the "Growing" SLOCA is 1×10^{-5} per year.

Frequency of the Event Leading to Core Damage. Combining the frequency of the EFC and the probability of the HFEs yields an estimate of core damage frequency due to the physical deviation of the "Growing" SLOCA scenario creating an EFC that sets up the operators for failure. To have failure, either the operators fail to restart RHR pumps or they successfully start the pumps and fail to complete the sump recirculation cooling lineup before the RWST runs dry; i.e.,

$$P(UA_1) + \{[1 - P(UA_1)] * P(UA_2)\} = 0.35.$$

Combining the frequency of the EFC with the probability that one of the UAs occurs yields a core damage frequency of 3.5×10^{-6} per year for the "Growing" SLOCA deviation case.

E.10 Issue Resolution

This ATHEANA example analysis was performed to address one specific issue:

> *Can reasonable variations on the SLOCA scenario be identified, such that progress through the EOPs is significantly more difficult than for the SLOCA of the FSAR safety analysis?*

The analysis defined several deviation scenarios in Table E.5 and expanded in Table E.9 that go beyond training and FSAR analysis and could lead to core damage. They all increase the difficulty of progressing through the EOPs compared to the SLOCA of the FSAR. However, they are not equally "reasonable." We consider each of the four deviation cases separately in the following paragraphs.

---

[10]Current thinking is that the frequency of the DBA LLOCA must be much less than estimates used in most PRAs, including ours. Addressing that issue is beyond the scope of the current analysis. We note, however, that a most likely estimate much lower is not inconsistent with a 1×10^{-4} per year average frequency, if the average comes from slightly higher than average frequency in very small number of pipes, with significant flaws present due to fabrication, construction, operational, or maintenance-related damage.

E.10.1 "No" SLOCA Deviation Case: Reduced ECCS Flow

The key issue in this case is that an expected response to a scenario modeled in all PRAs is less direct and more time constrained than is generally assumed in the existing analyses. The functional restoration guidelines are in general not as direct as the normal EOPs and are performed under greater time constraints and higher anxiety. Moreover, some of the actions are last ditch efforts; operators get only one chance to do them correctly. This is pointed out in EOP back up documents, but is not always a strong focus. Our sense is that HRA of all functional restoration (FR) procedures might identify cases where a more direct approach to responding to equipment failures would be helpful.

E.10.2 "No" SLOCA Deviation Case: Pressurizer Steam Space SLOCA

The key lesson from this deviation case is that, even when the EOPs "work," there are entry conditions (deviations) that, while related, are different enough to go unrecognized by the operators. Then the high level of training on the more likely, or more expected, scenarios can create a bias against following a helpful EOP, because the common, related conditions are not recognized.

In this particular case, a better understanding of phenomena associated with voiding would be helpful.

E.10.3 "More" SLOCA Deviation Case: Break Size Greater than DBA SLOCA

In this case, the scenario becomes very difficult, because of the misleading readings. From observations of drills on similar scenarios, the scenario difficulties would not be so easily addressed in EOPs as in plant operations practice. An approach that relies on collegial agreement among operators and encouragement to speak one's mind when the situation is not well understood would seem to offer the best hope for unraveling such a convoluted scenario. The EOP is something of a trap until the problems with pressure (somewhat easy to dismiss due to previous problems) and subcooling margin are understood. And they are unlikely to be seen until someone in the control room mentions to their colleagues that there are inconsistencies in the scenario.

We note that plots of trends in parameters could highlight the inconsistences and that the team in the technical support center are likely to do this, even if the control room operators do not. Nevertheless, it is not a convincing solution and it may be limited to specific cases. The collegial approach to operations provides a more robust solution.

E.10.4 "More" SLOCA Deviation Case: "Growing" SLOCA

The remaining case, the "Growing" SLOCA, involves many challenging aspects. The probability of an HFE, given the scenario, is quite high. In a generic sense, the frequency of this initiator is very low. Nevertheless, there are several reasons to consider the case seriously:

- It is more than frequency. In the spirit of medical diagnosis, it is not simply the probability of a possible diagnosis that is of interest. If some very high consequence *treatable* disease has a low probability of being correct, we hope our physician does not dismiss it because of its low probability, but investigates further (more research on the characteristics of the disease, more tests, etc.). We are more willing to play the odds, if the consequences are low. This is not to say that risk is not a suitable criterion for programmatic decision making, but that in diagnostics, it is worthwhile digging deeper and being better prepared for high consequence events.

- The frequency might not be correct. There may be failure modes not yet evidenced that can occur under specific conditions, including aging. Even if generically the chance of the "Growing" SLOCA may be very low, specific plants with specific designs, operating histories, maintenance histories, and vulnerabilities could have a much higher frequency for such events.

- Similar events. As identified in Table E.6, a LLOCA that plugs and later expands could have similar consequences. Other possibilities include a smaller, more likely LLOCA combined with

- One RHR pump out of service and a second that was allowed to run "too long" in the operators' view such that they believe it is damaged.

- Channel B pressure instrument out of service and the operators disbelieve channel A (as in the greater than DBA SLOCA case.

Thus the issue resolution process may demand that the analysis be extended or that, because of the broad range of possibilities, some precautions in training or practice be instituted to ensure, if an unlikely or unforeseen condition arises, the operators are well prepared to deal with it.

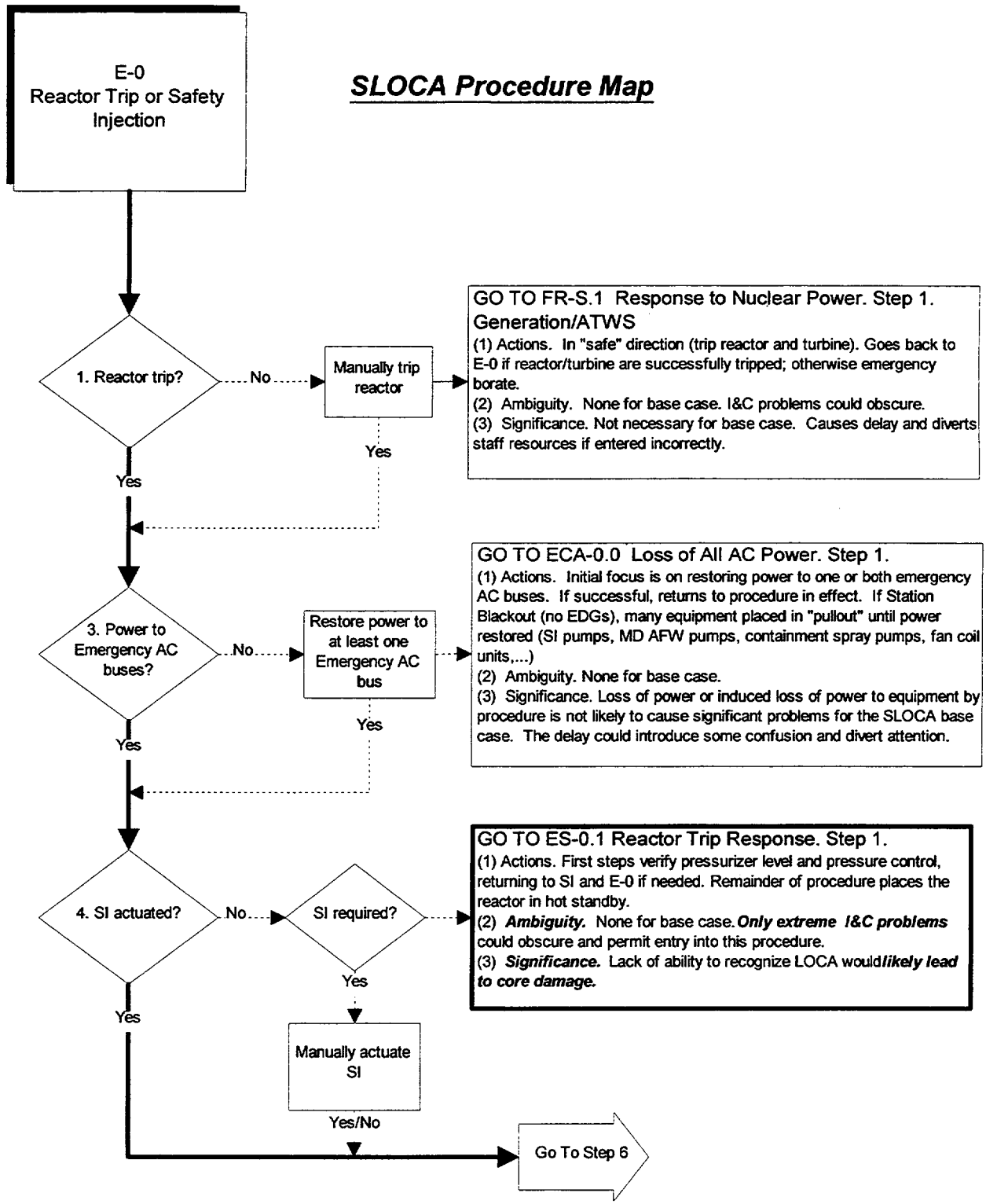


Figure E.12 EOP Map of Base Case SLOCA (Sheet 1)

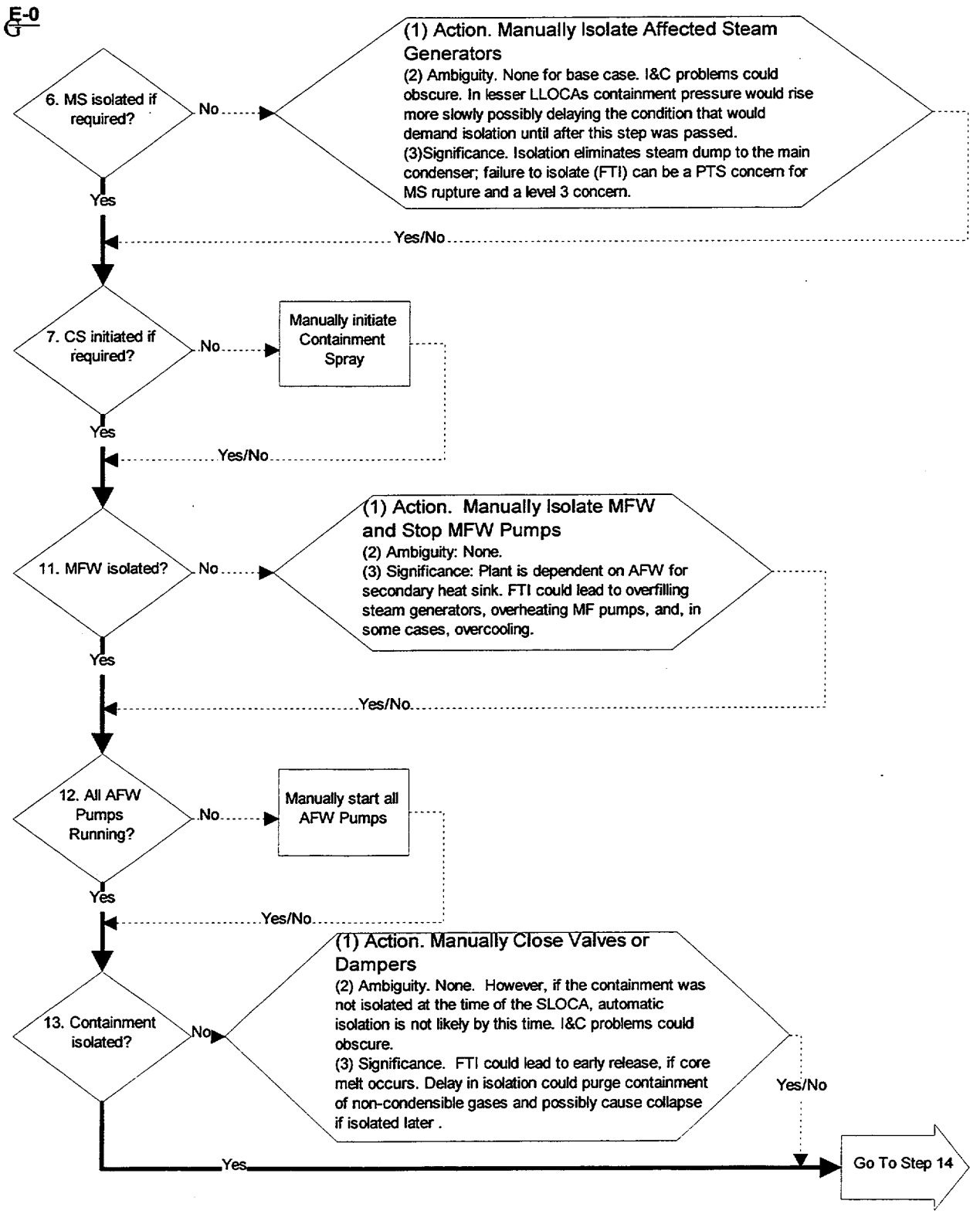


Figure E.12 EOP Map of Base Case SLOCA (Sheet 2)

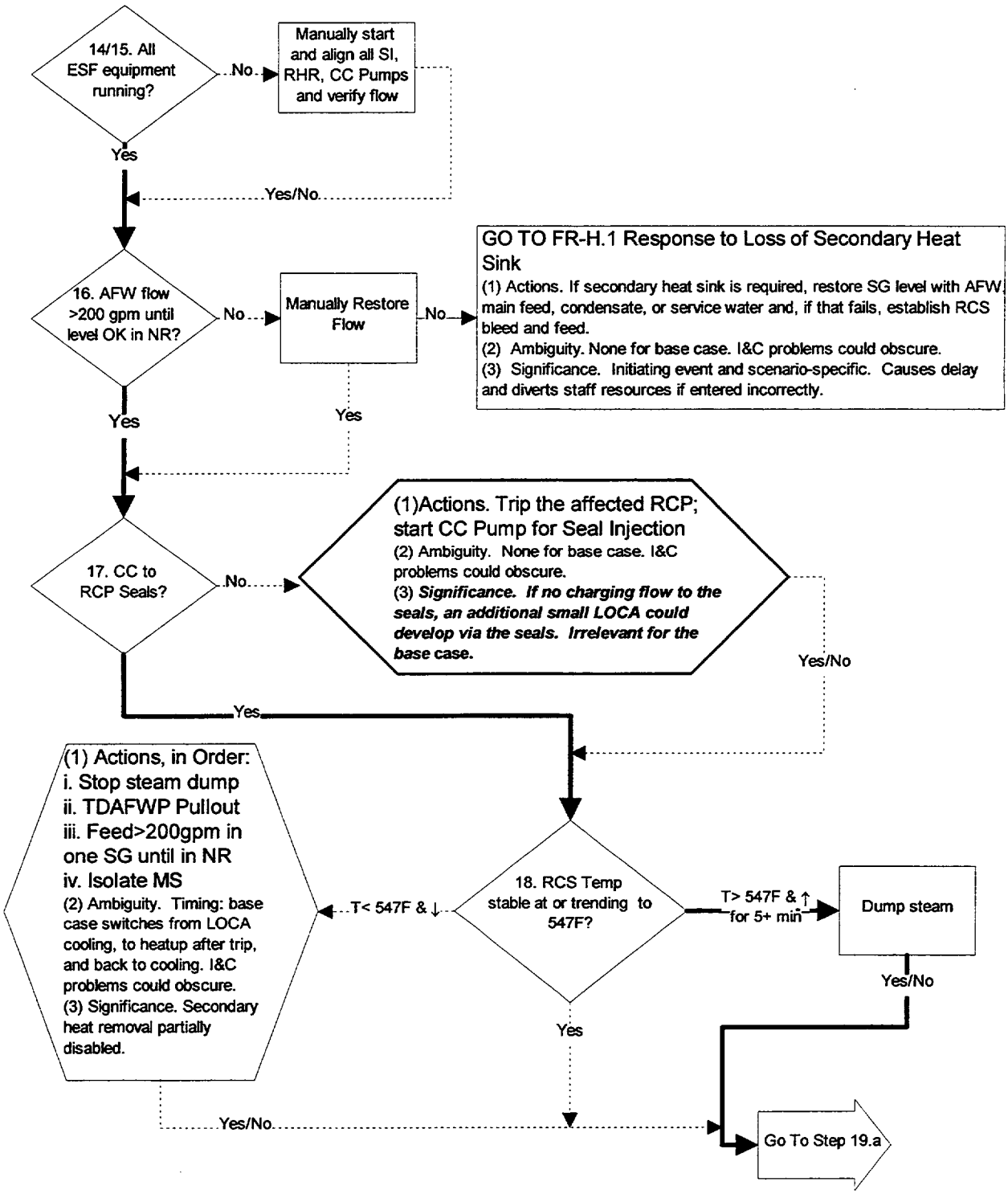


Figure E.12 EOP Map of Base Case SLOCA (Sheet 3)

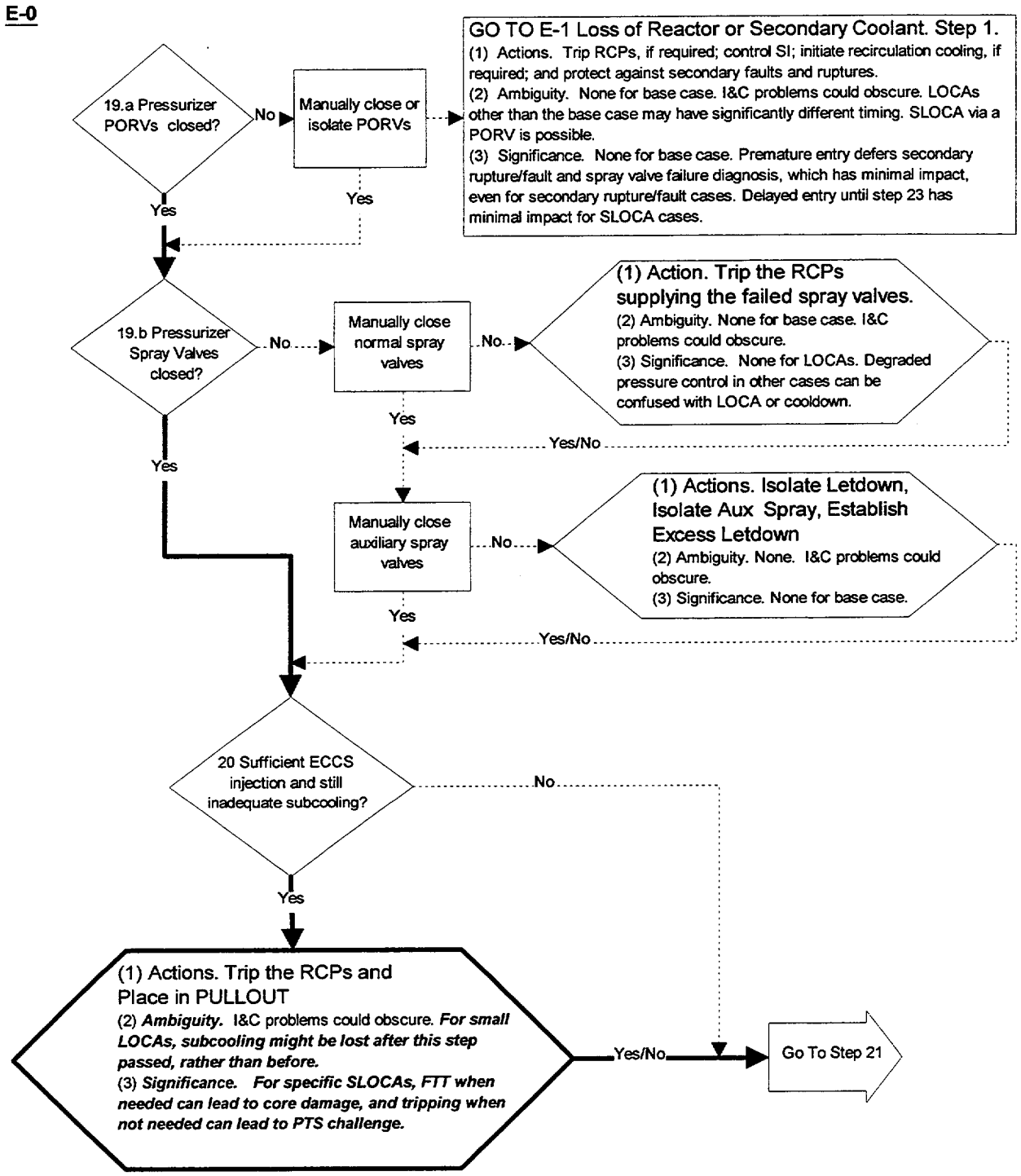


Figure E.12 EOP Map of Base Case SLOCA (Sheet 4)

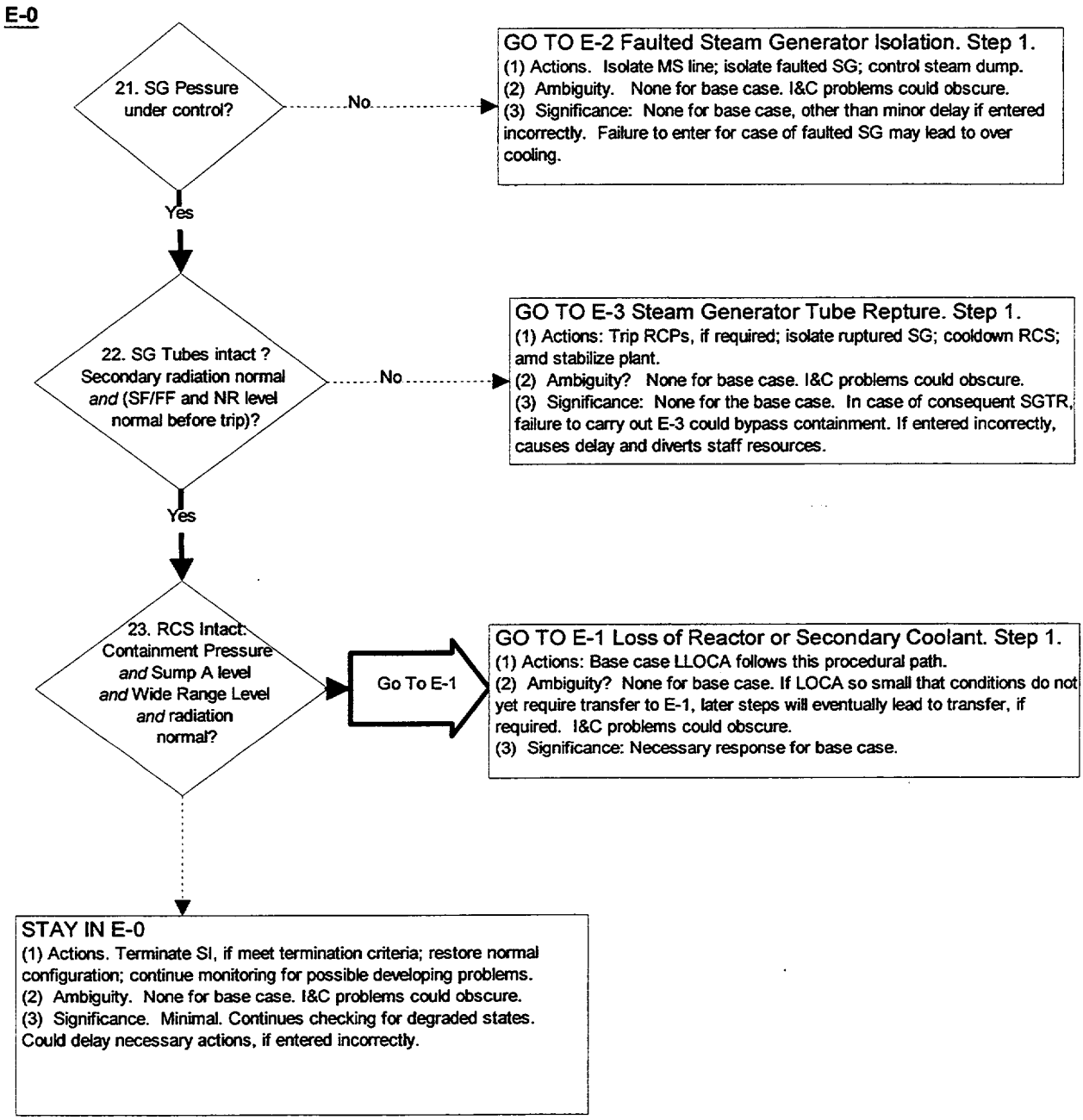


Figure E.12 EOP Map of Base Case SLOCA (Sheet 5)

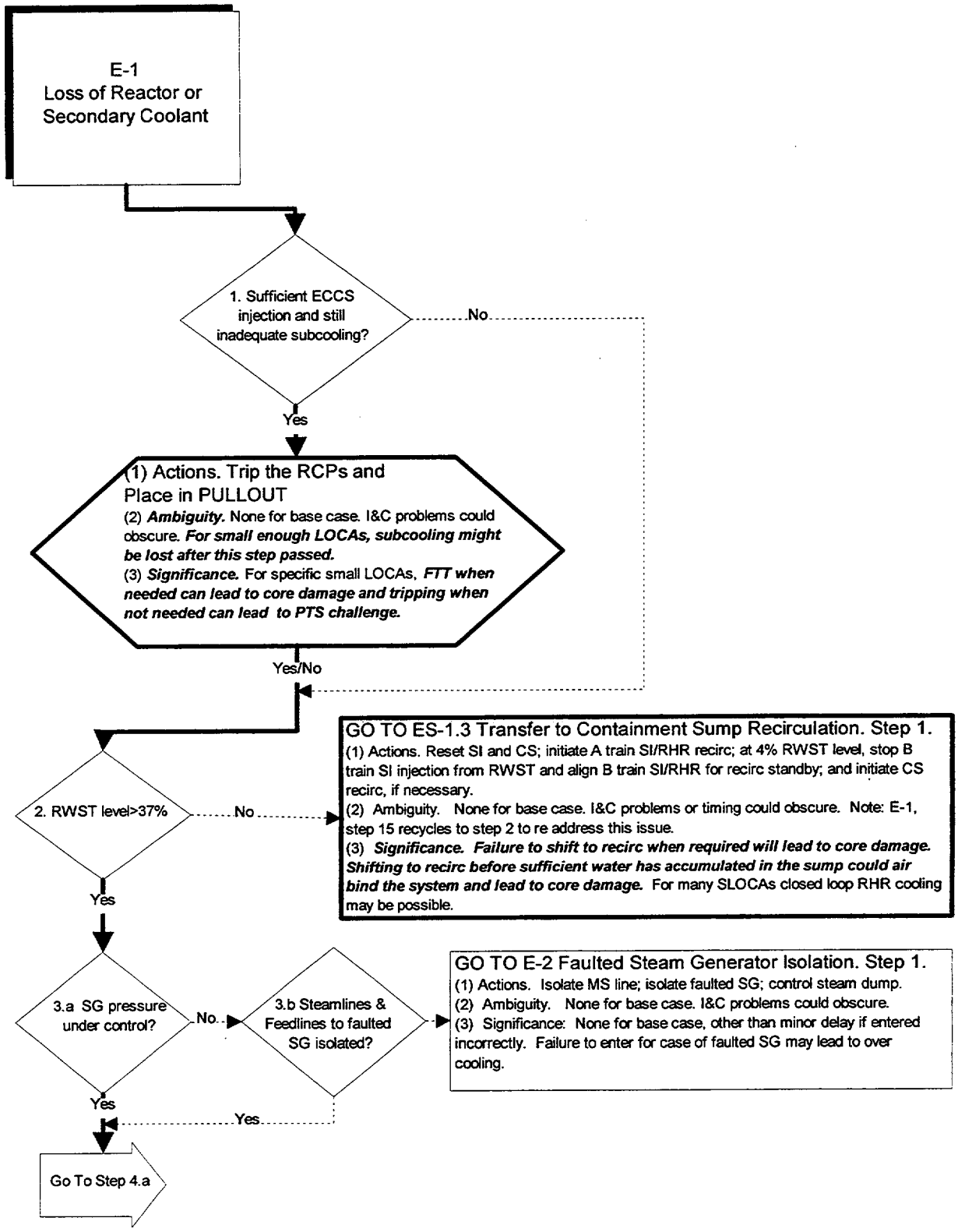


Figure E.12 EOP Map of Base Case SLOCA (Sheet 6)

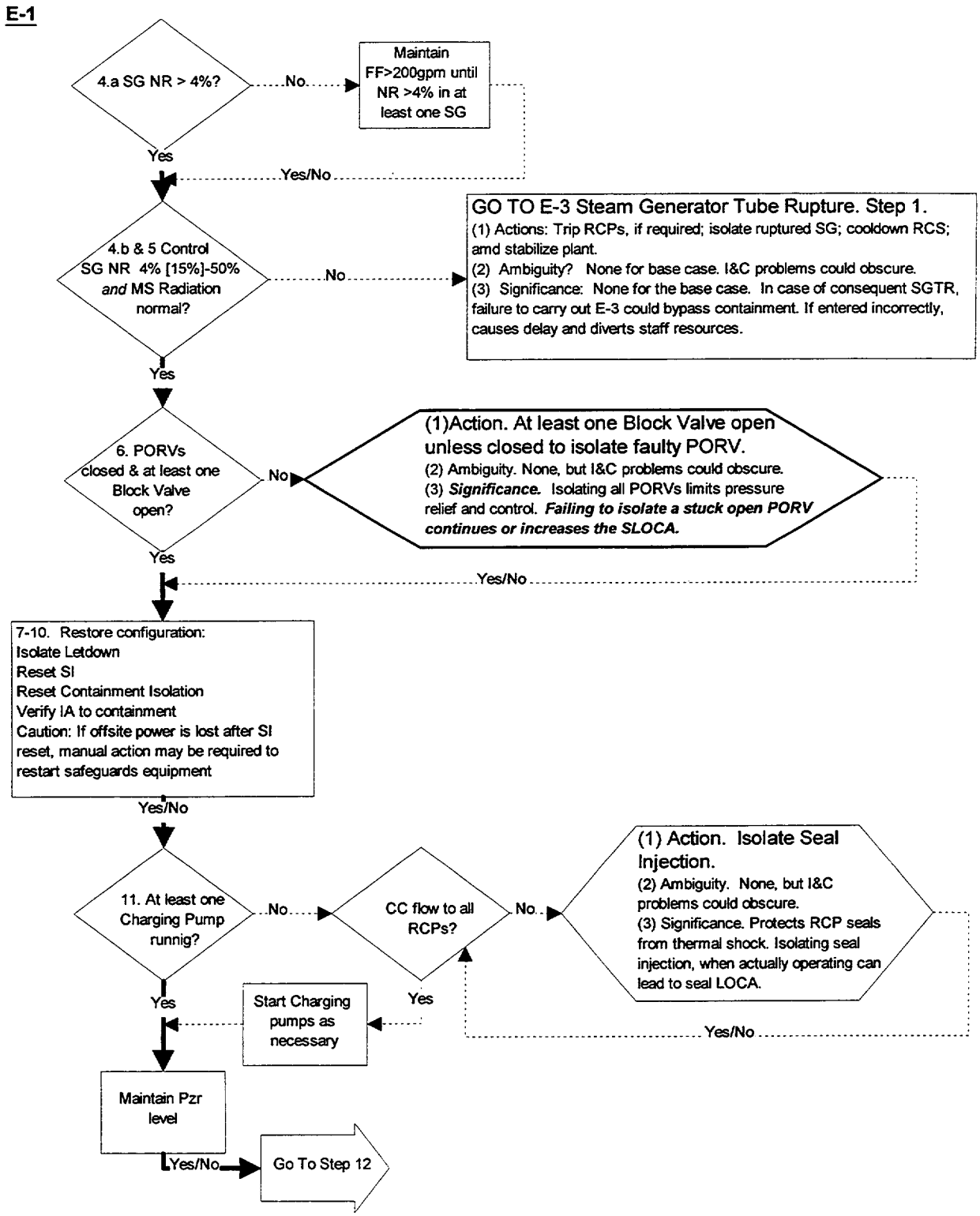


Figure E.12 EOP Map of Base Case SLOCA (Sheet 7)

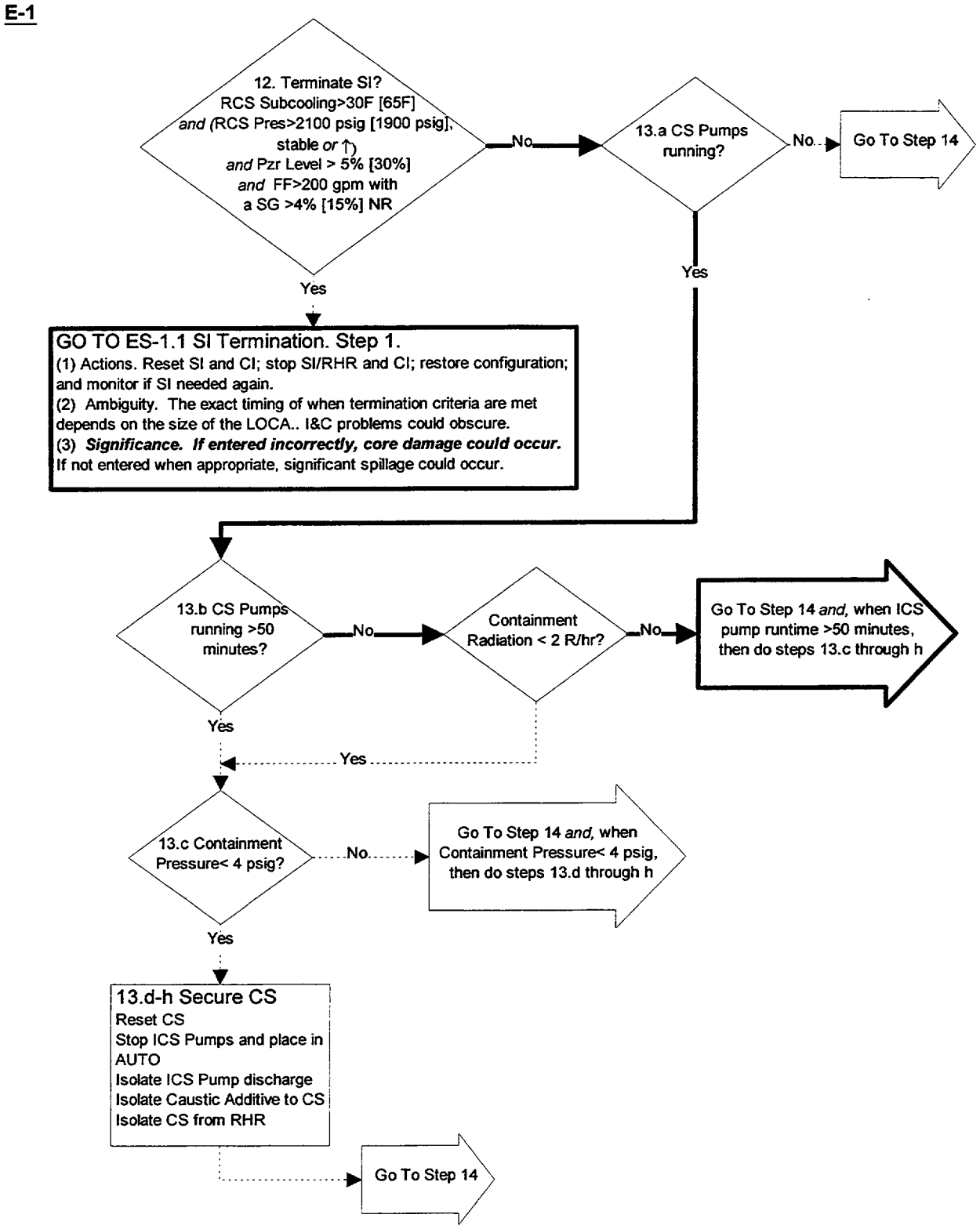


Figure E.12 EOP Map of Base Case SLOCA (Sheet 8)

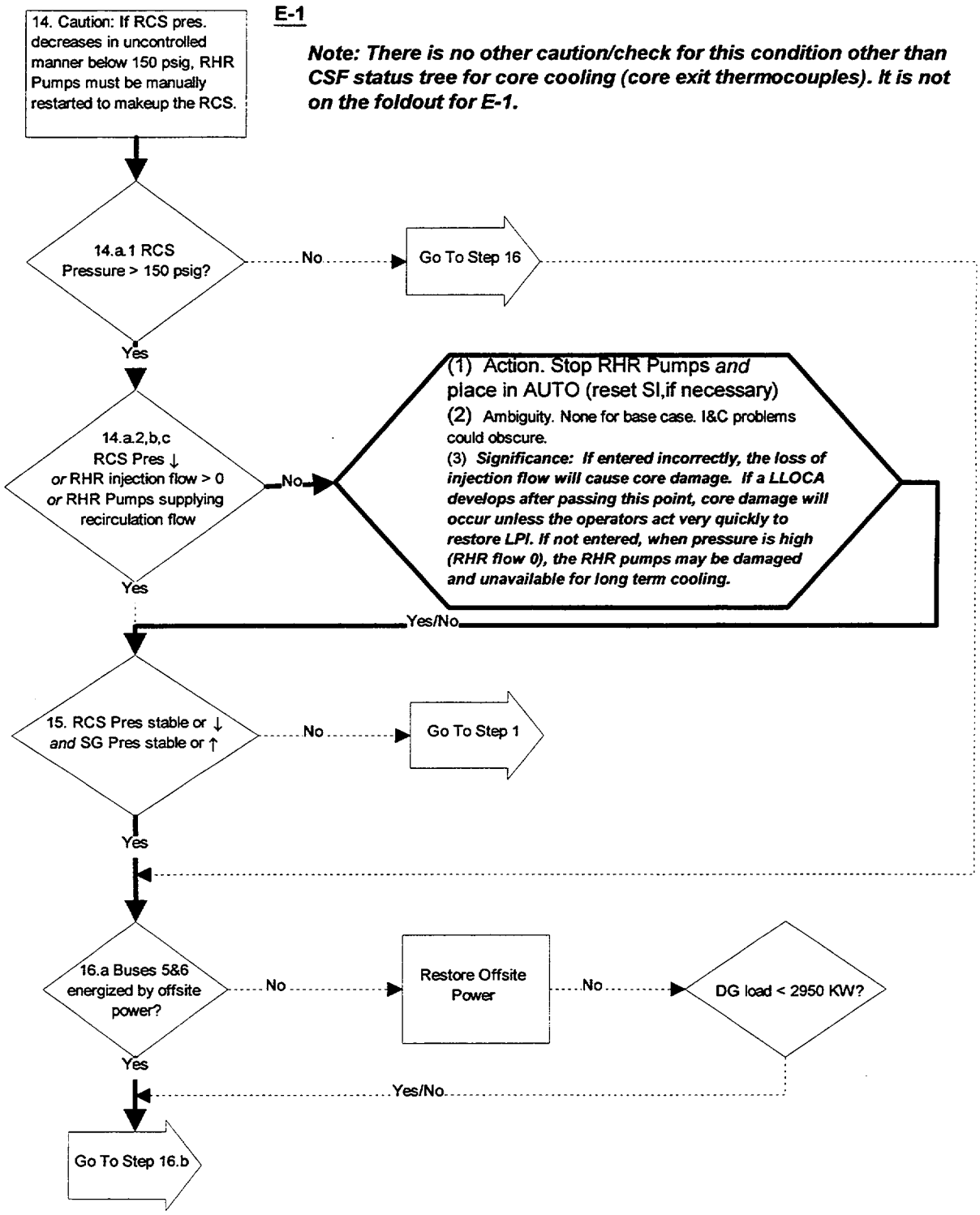


Figure E.12 EOP Map of Base Case SLOCA (Sheet 9)

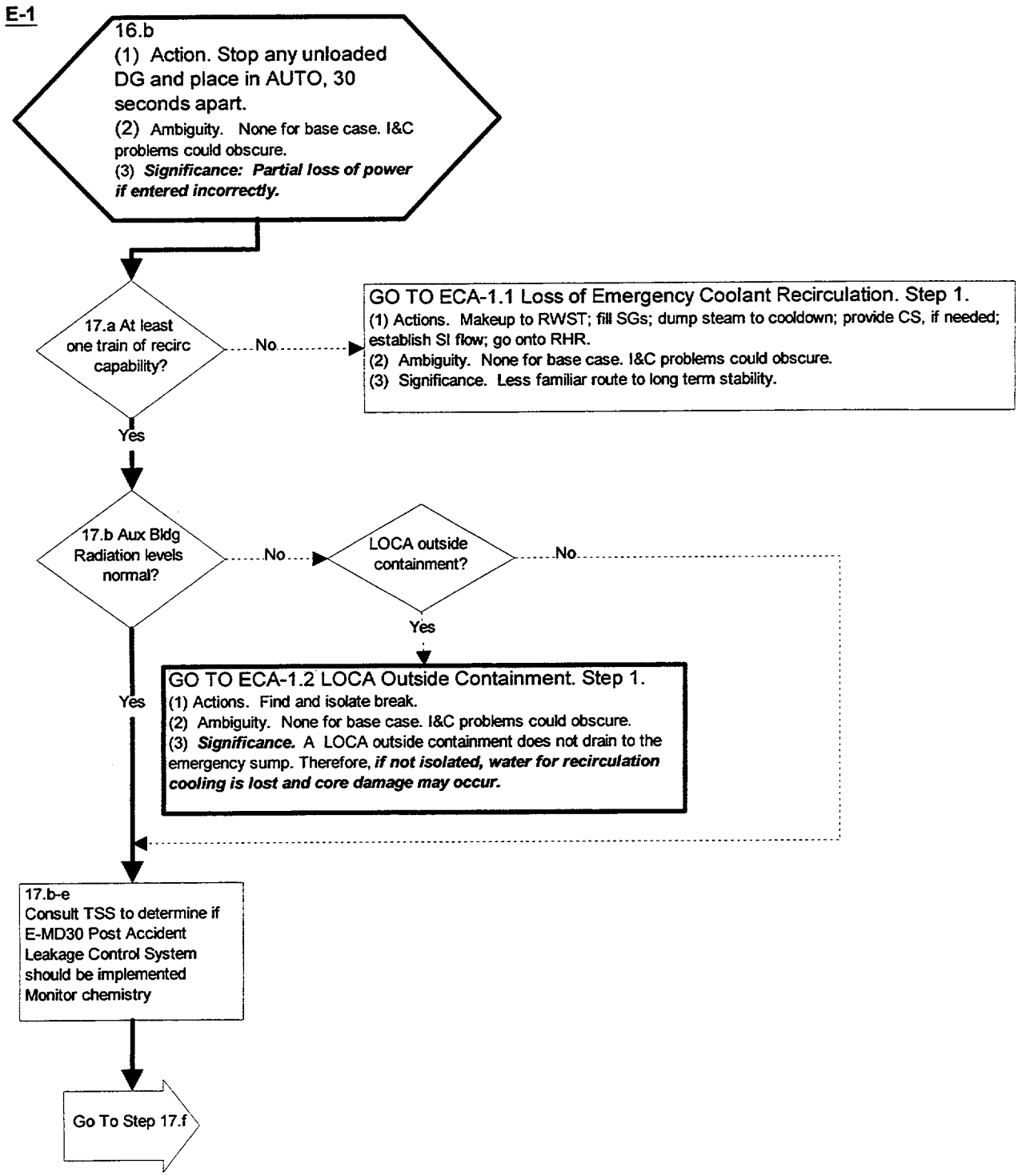


Figure E.12 EOP Map of Base Case SLOCA (Sheet 10)

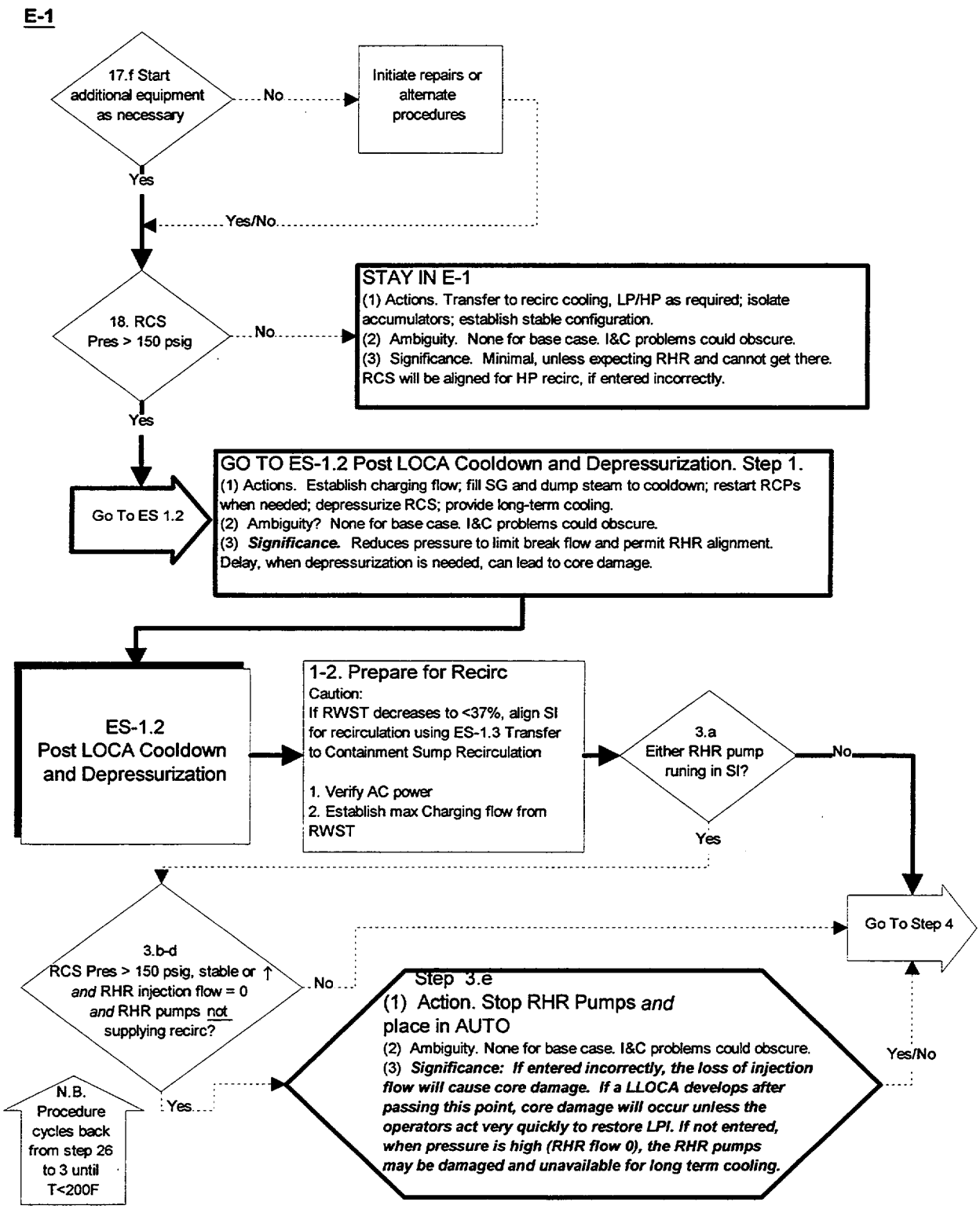


Figure E.12 EOP Map of Base Case SLOCA (Sheet 11)

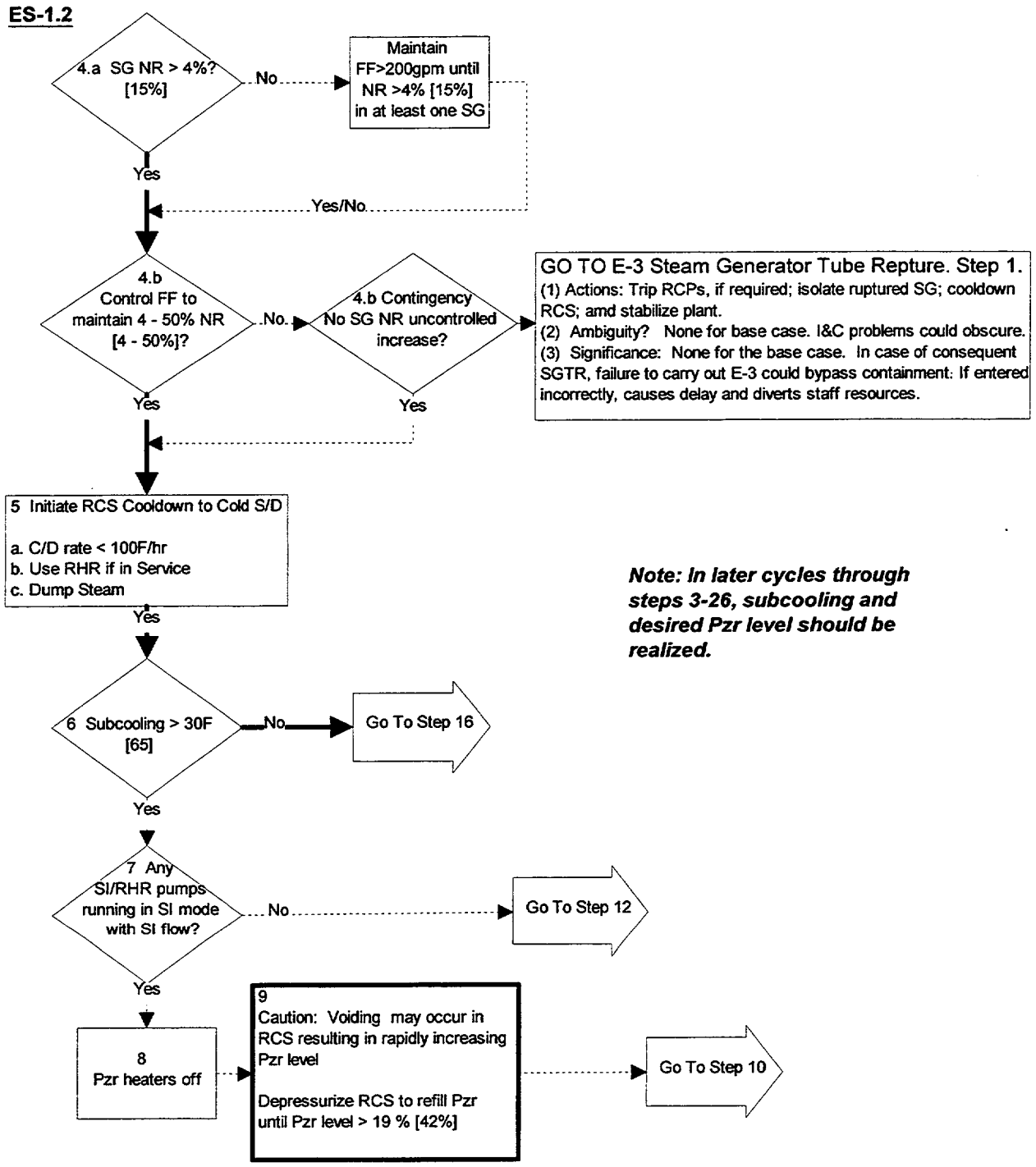


Figure E.12 EOP Map of Base Case SLOCA (Sheet 12)

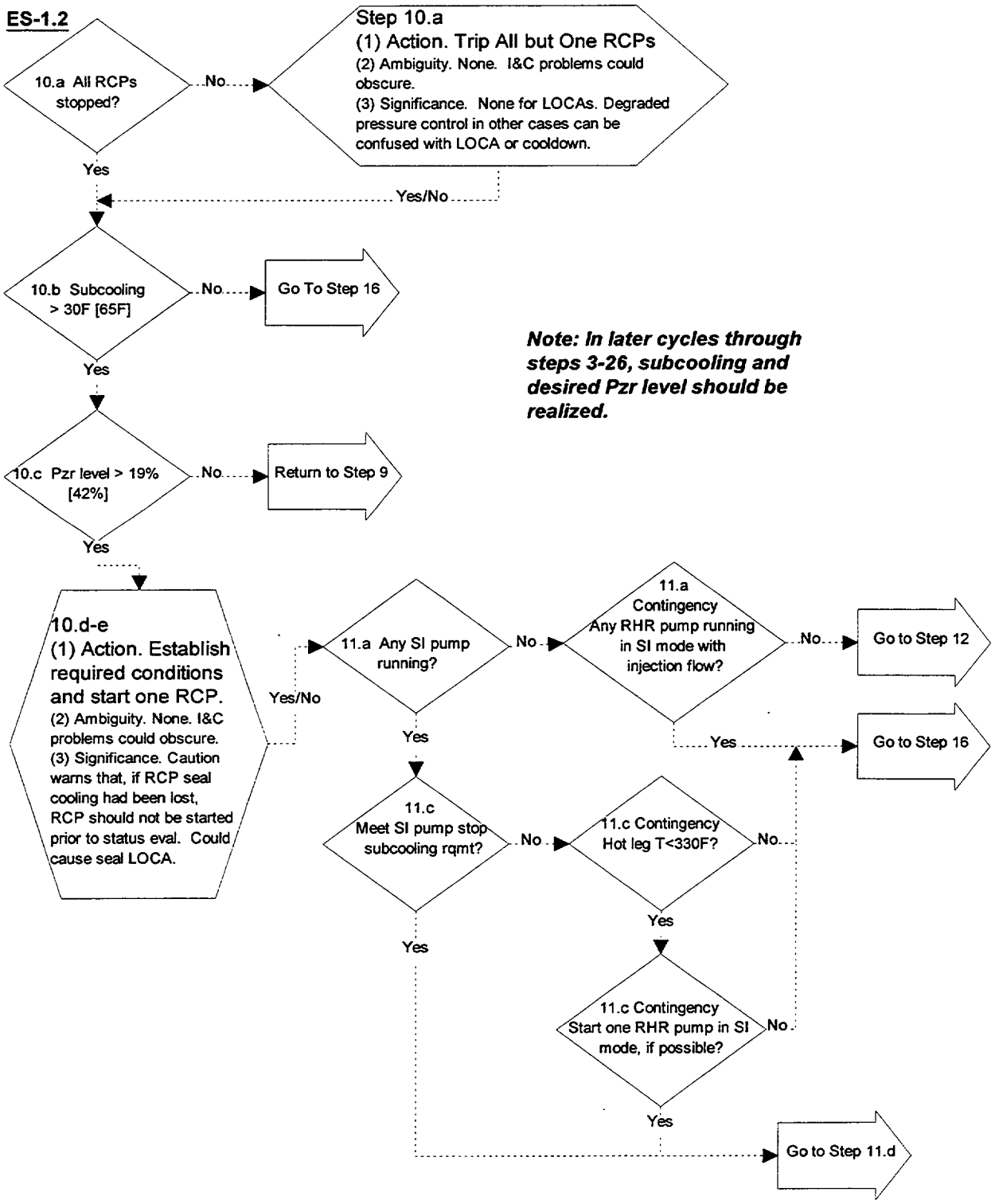


Figure E.12 EOP Map of Base Case SLOCA (Sheet 13)

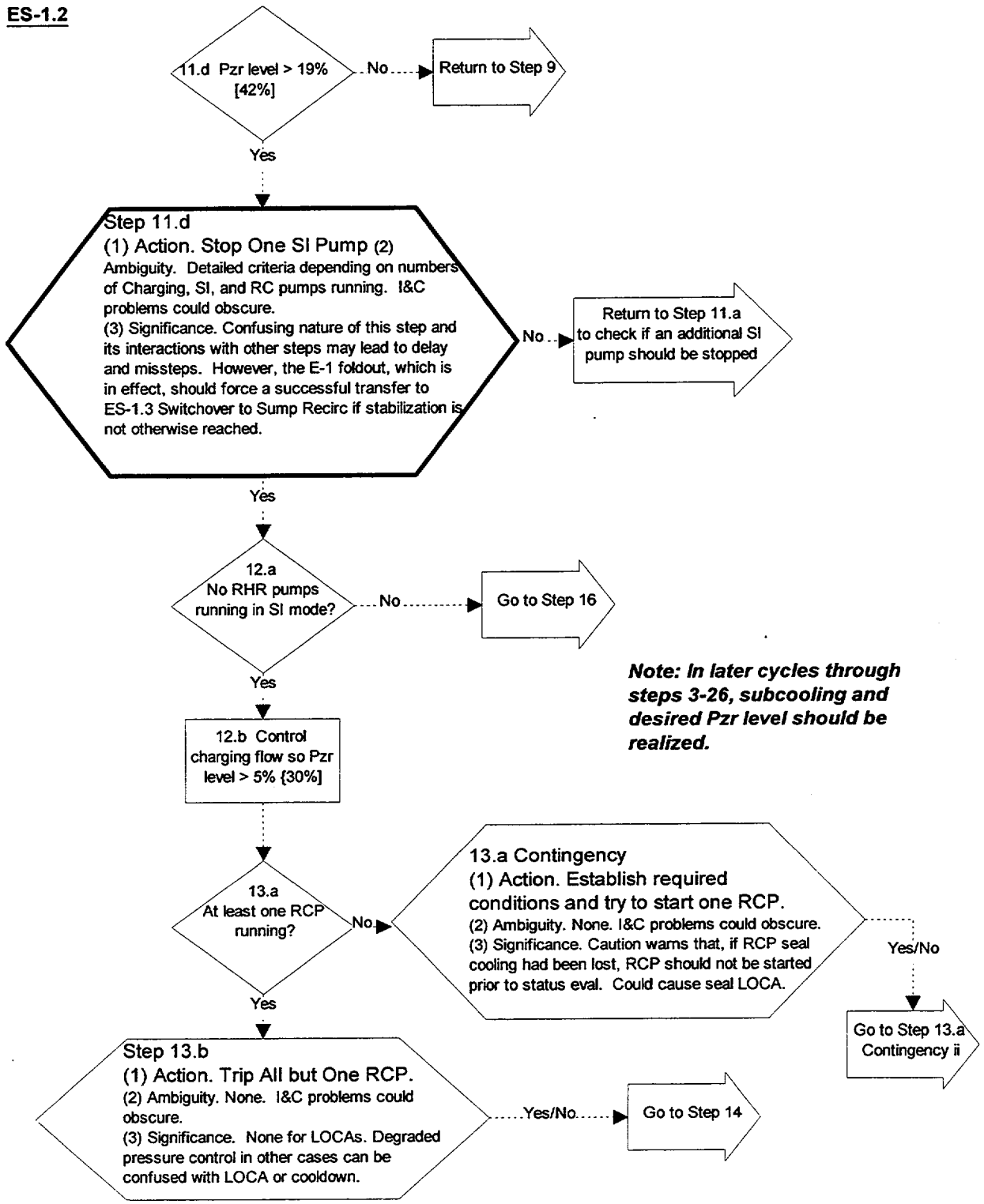


Figure E.12 EOP Map of Base Case SLOCA (Sheet 14)

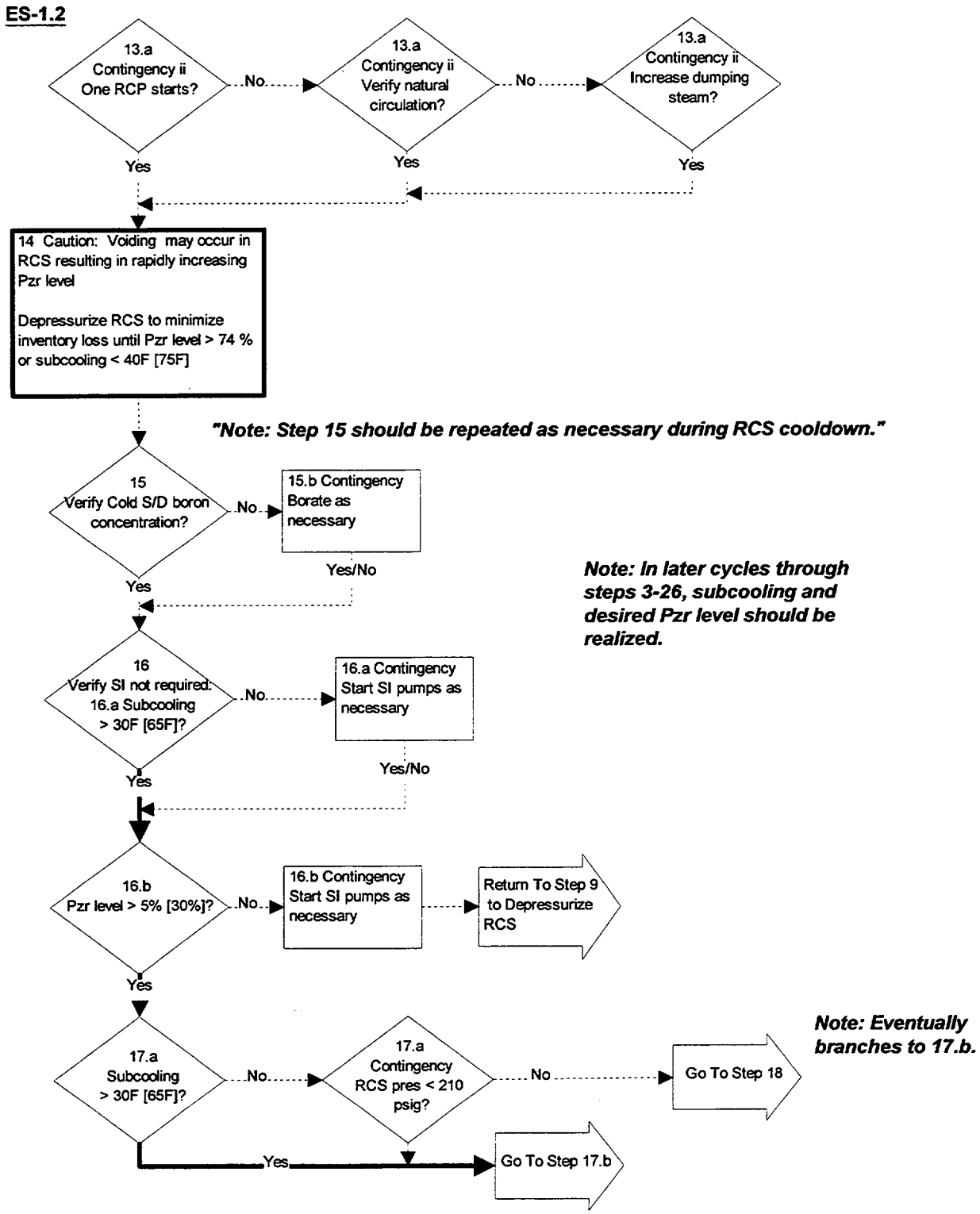


Figure E.12 EOP Map of Base Case SLOCA (Sheet 15)

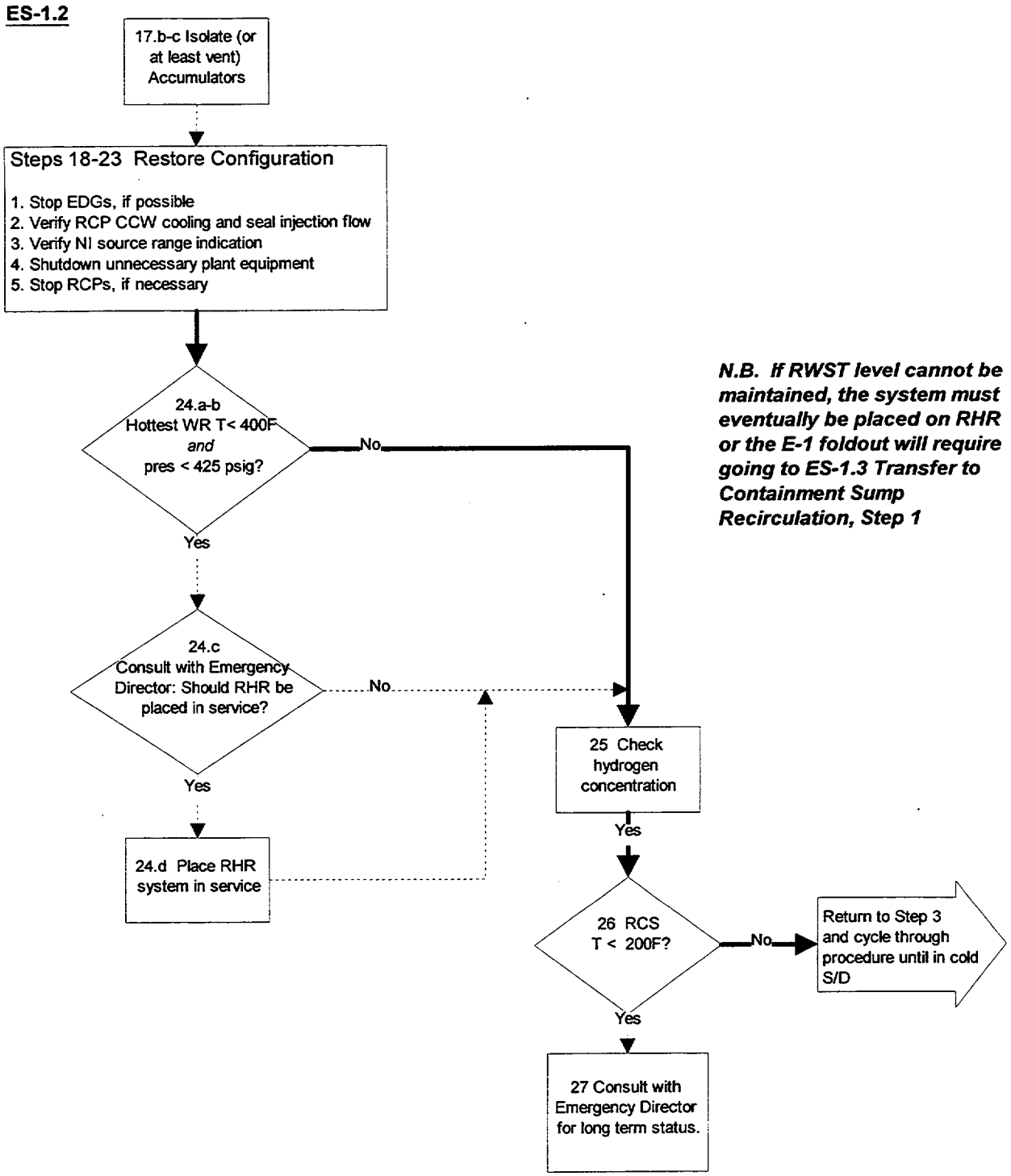


Figure E.12 EOP Map of Base Case SLOCA (Sheet 16)

APPENDIX F
DISCUSSION OF COMMENTS FROM A PEER REVIEW OF A TECHNIQUE FOR HUMAN EVENT ANALYSIS (ATHEANA)

(Paper appears in the *Proceedings of the 26th Water Reactor Safety Information Meeting*, NUREG/CP-0166, U.S. Nuclear Regulatory Commission, Bethesda, MD, 1998.)

Please note that comments described in this appendix were used to guide the revisions to ATHEANA contained in the main body of this report (NUREG-1624, Rev. 1).

Discussion of Comments from a Peer Review of A Technique for Human Event Analysis (ATHEANA)[1]

John A. Forester, Sandia National Laboratories
Ann Ramey-Smith, US Nuclear Regulatory Commission
Dennis C. Bley, Buttonwood Consulting, Inc.
Alan M. Kolaczkowski and Susan E. Cooper, Science Applications International Corp.
John Wreathall, John Wreathall & Co.

Abstract

In May of 1998, a technical basis and implementation guidelines document for A Technique for Human Event Analysis (ATHEANA) was issued as a draft report for public comment (NUREG-1624 [Ref. 1]). In conjunction with the release of draft NUREG-1624, a peer review of the new human reliability analysis (HRA) method, its documentation, and the results of an initial test of the method was held over a two-day period in June 1998 in Seattle, Washington. Four internationally known and respected experts in HRA or probabilistic risk assessment were selected to serve as the peer reviewers. In addition, approximately 20 other individuals with an interest in HRA and ATHEANA also attended the peer and were invited to provide comments. The peer review team was asked to comment on any aspect of the method or the report in which improvements could be made and to discuss its strengths and weaknesses. They were asked to focus on two major aspects: 1) Are the basic premises of ATHEANA on solid ground and is the conceptual basis adequate? 2) Is the ATHEANA implementation process adequate given the description of the intended users in the documentation? The four peer reviewers asked questions and provided oral comments during the peer review meeting and provided written comments approximately two weeks after the completion of the meeting. This paper discusses their major comments.

Introduction

In May 1998, a technical basis and implementation guidelines document for A Technique for Human Event Analysis (ATHEANA) was issued as a draft report for public comment (NUREG-1624

[1]This work was supported by the U.S. Nuclear Regulatory Commission and was performed at Sandia National Laboratories. Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the U.S. Department of Energy under Contract DE-AC04-94AL85000.

[Ref. 1]). In conjunction with the release of draft NUREG-1624, a peer review of the new human reliability analysis (HRA) method, its documentation, and the results of an initial test of the method was held over a two-day period in June 1998 in Seattle, Washington. Four internationally known and respected experts in HRA served as the peer reviewers. A brief description of the reviewers and their credentials follows:

- Dr. Eric Hollnagel - An internationally recognized specialist in the fields of human reliability analysis, cognitive ergonomics, cognitive systems engineering, and the design and evaluation of man-machine systems. Dr. Hollnagel is the author of more than 230 publications, including six books, articles from recognized journals, conference papers, and reports. In January 1998, he published a book entitled *Cognitive Reliability and Error Analysis Method (CREAM)*, which is itself a new HRA method. He is a member of the Swedish Reactor Safety Council and president of the European Association of Cognitive Ergonomics. Since 1995 Dr. Hollnagel has been principal advisor at the Organization for Economic Cooperation and Development (OECD) Halden Reactor Project, and since 1997 adjunct professor of Human-Machine Interaction at Linköping University, Sweden. He has a Ph.D. in cognitive psychology from the University of Aarhus, Denmark.

- Dr. Pietro Carlo Cacciabue - A sector head at the European Commission, Joint Research Centre, Institute for Systems, Informatics, and Safety, in Ispra, Italy. He has published more than 100 papers in professional journals and conferences and is the editor of a number of conference proceedings and books on safety assessment and human factors. Dr. Cacciabue serves as liaison for and holds a number of positions in several international organizations, such as: the International Association for Probabilistic Safety Assessment and Management (director since 1993), consultant for the Direction Générale Aviation Civile, France (since 1994), Institution of Nuclear Engineers, UK, (member since 1984), European Safety Reliability and Data Assoc. (executive committee member 1992-1995), and the European Association of Aviation Psychology (member from 1996 to the present). He has a Ph.D. in nuclear engineering from Politecnico di Milano, Milan, Italy.

- Dr. Oliver Straeter - A researcher for Gesellschaft fur Anlagen und Reaktorsicherheit (GRS) in Germany in the Safety Analysis and Operational Experience Branch. He was a researcher at the RWTH in Aachen and the Ruhruniversität in Bochum and also worked at Siemens Nixdorf AG compiler laboratory in Munich. Dr. Straeter has published several journal articles in the area of human reliability, including a recent article in *Reliability Engineering and System Safety* (Vol 58, 1997), entitled "Human-Centered Modeling in Human Reliability Analysis: Some Trends Based on Case Studies." Dr. Straeter holds a Ph.D. in human engineering psychology from Technical University of Munich.

- Mr. Stuart R. Lewis - A consultant specializing in the application of reliability and quantitative risk analysis methods. Mr. Lewis is the president of Safety and Reliability Optimization Services (SAROS), Inc., Knoxville, TN, which he co-founded in 1984. Examples of current and past relevant work include assisting nuclear licensees in updating and maintaining their

probabilistic safety assessments (PSAs) and updating the HRAs for the PSAs of several licensees. He has also assisted the Oak Ridge National Laboratory by reviewing analyses performed under its Accident Sequence Precursor Program, and is assisting Electricité de France in keeping abreast of technical and regulatory developments concerning severe accidents. He performed the HRA portion of several of the probabilistic risk assessments (PRAs) performed by nuclear power plant licensees for the U.S. Nuclear Regulatory Commission's Individual Plant Examination program. Mr. Lewis holds both B.S. and M.S. degrees in nuclear engineering from Purdue University.

In addition, approximately 20 other individuals with an interest in HRA and ATHEANA also attended the peer review meeting and were invited to provide comments. The peer review team was asked to comment on any aspect of the method or the report in which improvements could be made and to discuss its strengths and weaknesses. They were asked to focus on two major aspects:

(1) The soundness of the philosophy underlying ATHEANA. Are the basic premises on solid ground and is the conceptual basis adequate?

(2) Is the ATHEANA implementation process adequate, given the description of the intended users in the documentation? Assuming the technical basis is adequate, is the guidance for conducting the search and quantification processes and for integrating the results into the PRA adequate, for example, clear, effective, usable?

The four peer reviewers asked questions and commented orally during the peer review meeting. They also provided written comments approximately two weeks after the meeting. All of the reviewers indicated that the ATHEANA method had made significant contributions to the field of PRA/HRA, in particular by addressing the most important open questions and issues in HRA, by attempting to develop an integrated approach and by developing a framework capable of identifying types of unsafe actions that generally have not been considered using existing methods. The reviewers had many (and sometimes similar) concerns about specific aspects of the methodology and made many recommendations on ways to improve and extend the method and to make its application more cost effective and useful to PRA in general.

This paper discusses the major comments received from the peer review team and provides responses (but not necessarily resolutions) to specific criticisms and suggestions for improvements. A list of the general strengths and weaknesses of ATHEANA, as indicated by the reviewers, is provided first. Next, specific comments bearing on major aspects of the method are presented and discussed . Finally, general comments related to improving the efficiency and usefulness of ATHEANA are addressed.

General Strengths and Weaknesses of ATHEANA

The reviewers' general opinion of ATHEANA is that the method represents a significant improvement in HRA methodology; it is a useful and usable method; and it is a "good alternative

to first-generation HRA approaches." However, the method does not yet go far enough and therefore needs to be improved and extended. Several of ATHEANA's strengths, as indicated by the four reviewers, are listed below.

(1) "Until now, in my opinion, there is no other published approach that tries to solve the problem of including EOC [errors of commission] in PSA in such an extensive way. Other methods address only parts of this. Overall, the general approaches and concepts developed in the ATHEANA-method are appropriate to deal with the problem of EOC. I think that the ATHEANA-method as currently documented contains a lot of important aspects for understanding and integrating EOCs into PRA. However, many aspects are only mentioned implicitly. An explicit and concise elaboration is necessary to assure practicability..."

(2) "The real value of ATHEANA seems to be as a systematic way of exploring how action failures can occur. This is something that conventional HRA methods do not do well, if they do it at all, since they tend to focus on producing numbers. Although this use of ATHEANA does not really answer the need for an HRA approach, it might have a value in itself (as the comments from the demonstration participants expressed) and it might conceivably be decoupled from the HRA side. In that case a more streamlined method may be developed, that is less cumbersome to use. The demonstration of ATHEANA very clearly showed how it can be used to develop detailed qualitative insights into conditions that may cause problems, how it may generate a solid basis for redesign of working procedures, training, and interface, and how it may be used as a tool for scenario generation. Each of these are significant achievements in their own right."

(3) "The method described in ATHEANA is certainly well suited for overcoming the difficulties encountered when applying more classical human reliability methods and focuses on the important issues of context and cognition that need to be tackled. Many aspects of the methodology are commendable and give great added value to the whole methodology. In particular, the following features are important:

- the details in describing many processes and steps in the application of the methodology;
- the consideration for the crucial features that affect human cognition and behaviour in managing modern plants, included in concepts like the error-forcing context; and
- the identification of the appropriate retrospective approach for the evaluation of the factors influencing behaviour and basic data for prospectively analysing the likely outcome of erroneous behaviour and probabilities."

(4) "Properly applied, the methods that comprise ATHEANA should be able to yield significantly more insight into the nature of human actions that can contribute to the occurrence of a core-damage accident. These methods clearly provide a framework for

identifying some types of unsafe actions, and especially errors of intention, that would generally not have been considered using current methods. Moreover, they allow for a much more careful definition of the context and causes of these unsafe actions.

Without broader application of the methods, however, it is impossible to draw conclusions regarding the degree to which important actions that are not considered in present PRAs will be identified. It is reasonable to expect that some of the most important potential unsafe actions would be the result of subtle aspects relating to interactions among plant conditions or performance shaping factors that would be very difficult to postulate, even with the proper team makeup and extensive time available for the analysis.

What can be expected is that the methods will provide for the integration of understanding from the diverse team members that will lead to these new insights. This should be a synergistic process, allowing knowledge to be shared and captured in a way that enhances both the completeness and realism of the PRA, and the quality of training and procedures. A significant advantage of the method could be to provide a rationale for the characterization of the human failure events that often eludes us in present PRAs. While present methods may arguably yield reasonable quantitative results, they often fail to provide an understanding of the underlying causes of the human failures that are analyzed. Absent that understanding, it is very difficult to identify measures that can be taken to reduce the risk associated with unsafe actions. Consequently, it is often frustrating to identify a human action as risk-significant, but not to be able to give very satisfactory answers as to why, or what could be done to reduce that significance. With ATHEANA, on the other hand, the analysis of an unsafe action is necessarily truncated if an error forcing context cannot be identified."

The above statements clearly indicate that the ATHEANA method has made significant improvements in HRA methodology and that the method, as documented, is a useful and usable tool. Perhaps not surprisingly, current members of the ATHEANA development team (the authors of this paper) agree generally with the above statements. However, the reviewers were also very clear in indicating that, in their opinion, there are several important general shortcomings of ATHEANA. These are listed below.

(1) "There seems to be an inconsistency in the level of models being used, ranging from EOO-EOC (errors of omission - errors of commission) over the information processing model to the notion of slips and mistakes. It would be interesting to consider how the search process could be strengthened while relaxing the dependence on the model(s)."

(2) "There is no identifiable way of encompassing management and organization [M&O] factors or responding to the challenges of the broader socio-technical or contextual way of thinking (which also is seen by the conceptual problems in taking M&O factors into account in PSA)."

(3) "Insufficient consistency in the terms and concepts used, and significant differences between what is written in NUREG-1624 and what was said at the review."

(4) "The ATHEANA method is very cumbersome and presumably very costly. The guidance is too complex and depends too much on subject matter experts."

(5) "The quantification method is weak, and the quantitative results (of the demonstration) are unsubstantiated. The quantification is excessively dependent on expert judgement, hence possibly has low reliability as a method."

(6) "The qualitative results are good, but these might have been obtained in other ways, perhaps more efficiently. It is also doubtful whether a utility will undertake a significant effort just to get the qualitative results."

(7) "The implementation of the basic approaches is sometimes not elaborated far enough from my perspective. This makes the use of the method in the current status difficult and may cause high variance between different users. I also observed that the document NUREG-1624 and the presentations on the peer-review are sometimes not in accordance to each other. In order to have a usable and profound method, the basics has to be refined and extended."

(8) "Especially, I see the danger that the whole suggested procedure may fail if the role of the cognitive model (i.e. to work out and structure EMs [error mechanisms]) is not elaborated further. The cognitive model has a considerable effect on the consistency between EMs, the compatibility of prospective and retrospective analysis, the link between EFC [error-forcing context], EM and UA [unsafe actions] as well as the quantification procedure."

(9) "The methodology clearly presents a dilemma. Its effectiveness results from forming a diverse, experienced project team to perform a comprehensive, broad-ranging analysis. Few organizations, however, appear to be in a position to undertake such an extensive analysis without clearly defined, commensurate benefits. Thus, even if it is an excellent methodology from a technical standpoint, it will not be very valuable if it will not be used."

(10) "The potential wide application and popularity of the method are, however, associated with the *easiness of application* of the method and the *completeness* of the supporting information and data. The first issue (*easiness of application*) is related to the clear differentiation between retrospective and prospective analysis, which contains also the question of applicability of the cognitive model. The method, as presented in the report, generates some confusion, especially for non-specialists in human factors, even though one could argue that the ATHEANA team should contain such expertise. The question of the availability and *completeness* of a reference database and clear tables of parameters and variables sustaining the HRA approach has, in practice, already been almost completely tackled and solved. What remains to be done is simply the clear definition of the connections between such databases

and parameters on the one hand and models, paradigms and structure of ATHEANA on the other."

Although the above set of comments is not necessarily complete in regard to the limitations of ATHEANA as indicated by the peer reviewers, it is thought that the selected set does represent the more important general limitations identified by the reviewers. Some of the above criticisms are responded to directly, but in other cases, some future decisions are required. The criticisms and responses are grouped below according to major aspects of ATHEANA.

The ATHEANA Framework and Underlying Models

Two important aspects of the ATHEANA methodology are (1) the multi-disciplinary HRA framework (see Figure 2.1, NUREG-1624 [Ref. 1]) that describes the interrelationships between human error mechanisms, the plant conditions and performance-shaping factors (PSFs) that set them up, and the consequences of the error mechanisms in terms of how the plant can be rendered less safe, that is, UAs and (2) the human information processing or "cognitive" model (see Figure 4.1, NUREG-1624 [Ref. 1]) that is used to describe the human activities and mechanisms involved in responding to abnormal or emergency conditions and thereby assist analysts in searching for potential unsafe human actions. Several of the criticisms listed above (e.g., 1, 8 and 10) raise concerns about the descriptions and use of the framework and the cognitive model in ATHEANA. Essentially all of the peer review team had questions or concerns about these aspects of ATHEANA.

Regarding the multi-disciplinary HRA framework, several reviewers thought that the definitions and distinctions between the components of the framework and their interrelationships with each other and with the cognitive model were not sufficiently clarified. The reviewers considered this important because they correctly assumed that understanding the framework (and to some extent its relationship with the cognitive model) was important to understanding the ATHEANA methodological approach. One concern was exactly what was meant by "error mechanisms," how they are used in ATHEANA, and whether or not the terminology was appropriate, given the underlying assumptions of ATHEANA, for example, people usually behave rationally and are led to UAs as a function of the circumstances. Another concern was that the distinction between error mechanisms, PSFs and plant conditions was not sharp enough.

Clearly, "crisper" definitions of these terms are needed in the ATHEANA documentation because they are used to guide analysts in their search for UAs and the associated EFCs. One goal of using the construct of error mechanisms is to convey to analysts that there are human information processing activities that may be appropriate in some circumstances, but not in others. Examples of such activities are provided in the ATHEANA documentation and they are elaborated to some degree in the discussion of the cognitive model (Section 4 of NUREG-1624). The main purpose of the discussion in Section 4 is to encourage analysts to think about the potential for human error in a different manner than has been done in other HRA methods and not necessarily to provide a complete and validated set of error mechanisms. It is not obvious that further elaboration of possible error mechanisms will necessarily facilitate the ATHEANA search process or the quantification

process. Nevertheless, the clear use of the construct of "error mechanisms" in the context of ATHEANA will be addressed. To the extent that additional explanation and elaboration of potential error mechanisms will facilitate the search and quantification processes, such work will be performed for later revisions.

Consideration will also be given to a couple of reviewers' suggestion that the term "error mechanism" should be dropped because human information processing is probably not limited only by processing "mechanisms," which implies structures, (e.g., processing is probably also limited by inappropriate processing strategies) and because the behavior that leads to UAs is only an "error" in hindsight. As is assumed by ATHEANA, the information processing performed may have been perfectly appropriate in most situations and is inappropriate only because of special circumstances; it therefore is not an error in the usual sense. Recommendations for a replacement term for the construct included "behavior mechanisms" or simply "cognition."

As noted earlier herein, another concern expressed by the reviewers was with the distinction between plant conditions, PSFs, and error mechanisms. It was argued that it is not always easy to determine whether a particular factor belonged in one category or another (e.g., whether procedures and instrumentation problems should be categorized as plant conditions or PSFs) and that it was necessary for ATHEANA to make the distinctions clear. One reviewer indicated that the PSFs should be standardized and made complete. The current ATHEANA documentation has acknowledged that, in some cases, the distinctions are not always perfectly clear, but the emphasis from the analysis point of view is to ensure that the factors relevant to the EFCs are considered. Although it may be possible for the ATHEANA team to develop a useful underlying model for grouping the relevant factors and this effort may be attempted for revisions to the method, the main consideration in the application of ATHEANA is that as many relevant factors as possible are considered in identifying the EFCs.

Other issues regarding the models used in ATHEANA concerned the use of the EOC-EOO distinction, the slips versus mistakes categorization in the context of the other models used in ATHEANA (e.g., see criticism 1), and the ability of the method to correctly consider crew-related factors when the cognitive model generally applies to information processing by an individual. The latter concern suggests that it might be useful to include a "crew interaction" model that could be integrated with the cognitive model. The team will examine the feasibility and usefulness of such an endeavor.

Regarding the slips versus mistakes categorization, several reviewers argued that this categorization was probably not necessary and at least one argued that it was inappropriate. The use of such terminology, which does presume an underlying model not explicitly adopted by ATHEANA, will be addressed in future revisions.

Finally, several reviewers also suggested that the framework and models used in ATHEANA be compared to other more familiar models from existing methods in order to elucidate the differences between ATHEANA and other HRA approaches. This would certainly be a useful addition to the

ATHEANA report in that it would assist analysts in realizing the advantages to conducting an ATHEANA HRA. Clearly, revision of the ATHEANA documentation should discuss the uses and appropriate application of ATHEANA to various analysis tasks.

The ATHEANA Process

This section addresses a variety of important comments on aspects of the ATHEANA process.

Retrospective Analysis

The use of an ATHEANA-driven retrospective analysis of plant and other operational events was listed as one of the strengths of the ATHEANA process (see strength 3). More than one of the reviewers commented on the positive aspects of the use of retrospective analysis for assisting analysts in evaluating their plant and supporting the proactive HRA. In fact, their main concern was that a formalized, structured procedure, separate from the proactive search process detailed in ATHEANA, was not provided in the existing documentation. They suggested that a separate write-up and flow diagram be developed on how to perform retrospective analysis and on how it interfaces with the proactive analysis. Reviewers concerned with the definitions and relationships/connections between the elements in the framework and cognitive model also felt that clarification of these aspects would also greatly facilitate the retrospective analysis (see criticism 8). They argued for "taxonomies for actions, errors, and PSF" and clear rules for event decomposition in the retrospective analysis. In addition, they also suggested providing improved guidance on how to use the HERA database (Ref. 2) and the retrospectively analyzed events documented in Appendix B of NUREG-1624. [Note that HERA is a database being developed for the USNRC that contains documentation of significant events from nuclear and other industries. The events are represented from the ATHEANA perspective and in ATHEANA terminology.]

The ATHEANA team agrees that additional guidance on how to perform and use retrospective analysis and the HERA database would be useful additions to the ATHEANA documentation. Analysts would be able to learn more directly about the characteristics of ATHEANA and in addition to "self-training" on the ATHEANA "philosophy," framework, and models, they would better understand events that have occurred at their plant and how other events might occur in the future.

Prioritization Process

Several of the criticisms listed above (e.g., 4, 6, and 9) indicate that the demands of applying ATHEANA may be cost and time-prohibitive for many nuclear power plants. One aspect of ATHEANA that was developed in an attempt to allow users to focus their limited resources was a process for prioritizing the more important accident scenarios. While the reviewers generally were supportive of the prioritization process, several suggested that the process be further improved and proceduralized. Specifically, they wanted a "greater consideration of the risk potential of possible human failure events (HFEs)" and (on the basis of information provided at the peer review on the results of the trial application of ATHEANA) an earlier identification and assessment of crew

characteristics and other M&O factors that might make certain types of scenarios more likely to contain risk significant UAs than others.

Once again, the ATHEANA team agrees that improvements in the prioritization process, as suggested by the reviewers, would be useful. A characterization of the way plant crews interact with one another and approach accident scenarios would assist analysts in determining the types of scenarios likely to be problematic (see Appendix A, Section A.7, of NUREG-1624 for details). Explicit incorporation of other M&O factors (which is considered a weakness of ATHEANA; see criticism 2) at the prioritization stage may also be beneficial. It should be noted that there is nothing about ATHEANA that is inherently incompatible with the consideration of M&O factors (contrary to criticism 2). The main problems associated with accounting for M&O factors in ATHEANA are that there are no currently accepted methods for modeling such factors, and the costs associated with the additional analysis may offset the benefits.

In addition to these two items, there were several other comments related to the ATHEANA process that the ATHEANA team, in principle, agree with. They include the following:

- Provide further guidance for the creative thinking/search process to lessen variability and interpretation, including providing guidance on how to "manage" group discussions. Also emphasize the need to document the process "as you go" and more closely link the documentation tables with the relevant sections of the search process.

- Stress more strongly the importance of modeling the support systems, in addition to the main safety systems, in searching for potential HFEs and UAs.

- Discuss to what extent dynamic reliability is or is not part of the process and why.

- Further stress where and how one treats organizational factors, team interactions, recovery, and dependencies

One additional comment on the ATHEANA process warrants a response from the ATHEANA team. It was suggested that there should be an explicit use of formal task analysis in conducting ATHEANA. While it is true that some of the existing HRA methods recommend the use of formal task analysis in order to understand the operators' tasks during accident scenarios, it is not clear that the additional costs associated with formal task analysis would necessarily be useful in applying ATHEANA. In conducting ATHEANA, the HRA team, using appropriate procedures, examines the crew's responsibilities during various accident scenarios and, when possible, conducts simulator exercises. It may be beneficial, however, to emphasize the step of carefully examining procedures relevant to particular accident scenarios early in the process of identifying potential UAs and their EFCs. This step is certainly part of task analysis and should assist analysts in identifying the more critical and likely UAs for further analysis.

The ATHEANA Quantification Process

The reviewers raised several issues associated with quantification. These include the overall ATHEANA approach of identifying and quantifying situations where the likelihood of failure is very high, the methods used to quantify a UA in a particular EFC, and the effect of the various PSFs and plant conditions on the likelihood of failure. Other comments pertained to the need to address recovery actions and dependencies in the quantification process.

A basic premise driving the development of ATHEANA is that the HFEs that have heretofore been most problematic for identifying and assessing their impact on plant risk are those in which a particular context creates a very high likelihood of failure. This premise is in contrast to the premise implicit in most other HRA methods that there is a constant (and usually low) likelihood of human failure for any given accident scenario. (It is true that some HRA methods have moved beyond this simple assumption, but they have not been widely used and have rarely been applied in a systematic way.) Therefore, the search process and the associated quantification process are principally aimed at identifying those conditions in which the UA probability will be much higher than in other non-forcing conditions. However, this fact does not imply that the application of ATHEANA would never identify situations in which the probability of the UA, given the EFC, is significantly less than 1.0. In such situations in which human error probabilities must be estimated, existing applicable HRA methods may be useful for quantifying the error probability, given the defined EFC.

Several reviewers suggested that the methods for estimating the probability of the UA be revised or broadened. We agree that alternative methods can be used. In the trial application, HEART (Ref. 3) was used because it most directly used conditions similar to those identified as EFCs in the scenarios, bearing in mind the data sources used in HEART and the level of description for the conditions under which the data were gathered. It is important to ensure that the method and data used to quantify the likelihood of an unsafe action in a particular EFC will be sensitive to those factors that create the forcing nature of the EFC conditions. An alternative approach that was suggested is to use a subjective-assessment method like SLIM-MAUD (Ref. 4). Such methods could be used in principle. However, the continuing difficulty is one of selecting appropriate anchor points for the assumed probability distribution. This problem has been raised previously in reviews of HRAs that have used methods like SLIM-MAUD in which the analyst provides the range within which a point probability is interpolated.

One reviewer suggested the use of tables for specific PSFs and plant conditions that showed their influence on the likelihood of unsafe actions. Such data could be derived from historical experience in the events reported in the database. However, this approach is at odds with the ATHEANA method, which considers the influence of PSFs and plant conditions to be an integral set of influences on performance, and not separable and discrete influences such as those reported in THERP (Ref. 5). In ATHEANA, the typical issue is "What combination of plant conditions and weaknesses in the displays, procedures, etc., has to occur to mislead operators into believing that action 'x' needs to be taken?" The key is that it is the combination, not each influence separately, that is important.

It is agreed that the analysis of recovery actions is problematic. In applying ATHEANA, the team has considered recovery on a case-by-case basis, looking specifically at ways the scenario may develop, where additional outside staff may become involved, and so on. The approach thus far has not been to treat recovery actions as separate from the initial UAs. Similarly, the method does not include explicit processes to model and quantify dependencies between actions. Clearly, future revisions and applications of ATHEANA must better address the analysis of recovery actions and dependencies.

Improving the Efficiency, Usefulness, and Consistency of ATHEANA

Several of the comments from the reviewers (e.g., criticisms 4, 6, and 7) express concerns about the resources required to apply ATHEANA and whether or not the obtained results will be important enough and complete enough for users to justify the costs. A related concern is whether the method has been specified in enough detail and "elaborated far enough" to allow consistency in the results obtained by different analysts applying the method. Similar concerns regarding resource demands and completeness were raised by the participants of the first demonstration of ATHEANA, which was held in 1997 at a pressurized water reactor nuclear power plant (see Appendix A, Section A.7, of NUREG-1624 for details).

The ATHEANA team acknowledges that a broad and careful application of ATHEANA will require significant resources. Although the search for important HFEs, UAs, and their EFCs will never be trivial, it can be manageable. Thus, steps will be taken to improve its efficiency (some of which are discussed below). Will the resources demanded by the method be worth it? ATHEANA will identify demanding accident scenarios and potential UAs and EFCs that could lead to serious accidents. Whether or not the method will identify numerous events that result in large increases in calculated plant risk metrics remains to be seen. Moreover, given the inadequacies of the HRA methods that were used to conduct the existing nuclear plant PRAs, it is impossible to know exactly what a realistic estimate of the baseline HRA contribution should be. Therefore, it is difficult to predict what kinds of changes in risk metrics to expect. In any case, the benefits of ATHEANA are much broader than those from performing revised PRA calculations alone. The improvements in HRA modeling to better identify operator vulnerabilities in accident scenarios and to better understand what are the contributors to operator performance will certainly be of significant benefit in assessing and managing plant risk. Nevertheless, it must be the case that the method can be applied without an excessive demand on licensee resources.

The peer reviewers and others identified several actions that will increase the effectiveness and efficiency of ATHEANA. These actions include the following:

- developing a computer-based user support system to guide the process and the documentation of the results,

- refining the prioritization process to facilitate identification of the types of scenarios and situations most likely to create problems,

- developing better guidance on when and how to develop and use simulator exercises to learn as much as possible about where and how unsafe actions can occur, and

- producing a "quick reference guide" that would allow analysts to bypass reliance on the NUREG document once they have some experience with the method.

Another issue raised by the peer reviewers concerns consistency in the application of the process and the potential for significant variability in results because of some of the "open-ended" aspects of ATHEANA, (for example, the creative thinking and brainstorming aspects of the process for identifying EFCs and the use of expert judgment in the quantification process). The ATHEANA team agrees that additional guidance is needed to ensure consistency in the results obtained using the method.

Finally, it should noted that reviewers of the method suggested that the documentation provide estimates of the costs and resources required to perform ATHEANA and that criteria should be provided for when ATHEANA should be used. While the former suggestion may be difficult to implement until additional tests of ATHEANA are completed, it is a reasonable suggestion. Providing a listing of criteria for when use of ATHEANA is called for would seem to be straightforward and will be considered for the revision.

Other Useful Suggestions

Several other comments received from the peer review team are worth noting because they are good suggestions that would improve ATHEANA. They include the following:

- ATHEANA should include an overview of PRA for participants without a background in PRA. Any training programs developed for ATHEANA could also provide such an overview, and aspects of PRA could be treated in more detail as the analysis progressed.

- It was recommended that a single "running" example be used while discussing the implementation process.

- It was recommended that additional examples for BWRs should be added. PWRs are overemphasized.

Conclusion

Taken together, the comments from the peer review team indicate that the work performed in the development of ATHEANA has resulted in significant contributions to the field of HRA and that ATHEANA is a viable HRA method. However, the reviewers also indicated that there were important clarifications and improvements that needed to be made to ATHEANA. Clearly, many of the recommendations made by the reviewers would, if implemented, make ATHEANA a better,

more effective, easier to use, and more "encompassing" methodology. However, a number of factors must be considered in determining which of the suggested changes are necessary, which would be useful but are not critical, and which would be useful but are currently impossible. The development of an HRA method such as ATHEANA is certainly limited by the state of current knowledge in a number of domains such as cognitive psychology, crew dynamics, and management and organizational factors. In addition, the unavailability of actual data from crew performance in nuclear power accidents or from other domains that might be generalized to control room performance certainly limits the ability of any HRA method to precisely predict performance. Other factors include the danger of over-complicating the method in attempts to be more precise and complete. It seems to the ATHEANA team that the most important goal is to provide a usable method that is as cost-effective as possible -- one that will allow analysts to identify, understand as much as possible, and quantify as accurately as possible, potential unsafe human actions that could lead to serious accidents in nuclear power plants or other domains. The explicit procedures, information, and guidance provided in ATHEANA certainly provides HRA analysts with a new and explicit set of tools to achieve this goal. To the extent viable changes recommended by the reviewers will further this goal, in particular by making the method more valid and easier to use, attempts will be made to incorporate them into the ATHEANA methodology.

References

1. U.S. Nuclear Regulatory Commission, *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis, Draft Report for Comment* , NUREG-1624, Washington, DC, May 1998.

2. S. E. Cooper, W. J. Luckas, and J. Wreathall, *Human-System Event Classification Scheme (HSECS) Database Description*, BNL Technical Report No. L2415/95-1, Brookhaven National Laboratory, Upton, NY, December 1995.

3. J. C. Williams, "A Data-based Method for Assessing and Reducing Human Error to Improve Operational Performance," 1988 IEEE Fourth Conference on Human Factors and Power Plants, Monterey, California, IEEE, 1988.

4. D. E. Embrey, et al., "Slim-Maud: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment," Vols. 1-2, NUREG/CR-3518, U.S. Nuclear Regulatory Commission, Washington, D.C., March 1984

5. Swain, A.D., and H.E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, Rev. 1, Sandia National Laboratories, Albuquerque, NM, August 1983.

APPENDIX G
GLOSSARY OF GENERAL TERMS FOR ATHEANA

GLOSSARY OF GENERAL TERMS FOR ATHEANA

Availability Heuristic : The tendency of individuals to base interpretations or judgements on the ease with which relevant information can be recalled or with which relevant instances or occurrences can be imagined. Availability can be influenced by factors such as the recency and salience of the individual's own experiences.

Circumvention: A deliberate, deviation from rules and practices that has the intention of maintaining safe and/or efficient operations.

Cognitive Activity: Cognitive activity is the thought process associated with the operator's (1) situation assessment, (2) monitoring and detection, (3) response planning, and (4) response implementation.

Cognitive Factors: Cognitive factors affect the quality of output of major cognitive activities and therefore, affect operator performance. Three classes of cognitive factors are knowledge, processing resource, and strategic factors. Errors arise when there is a mismatch between the state of these cognitive factors and the demands imposed by the situation.

Confirmation Bias: The tendency of individuals to seek or interpret indications in ways that confirm expectations. The result can be a failure to appropriately revise opinions or interpretations in light of new, conflicting information.

Error-Forcing Context (EFC): The situation that arises when particular combinations of *performance shaping factors* and *plant conditions* create an environment in which unsafe actions are more likely to occur.

Error of Commission (EOC): A *human failure event* resulting from an overt, unsafe action, that, when taken, leads to a change in plant configuration with the consequence of a degraded plant state. Examples include terminating running safety-injection pumps, closing valves, and blocking automatic initiation signals.

Error of Omission (EOO): A *human failure event* resulting from a failure to take a required action, that leads to an unchanged or inappropriately changed plant configuration with the consequence of a degraded plant state. Examples include failures to initiate standby liquid control system, to start auxiliary feedwater equipment, and to block automatic depressurization system signals.

Error Mechanism (of humans): A psychological mechanism that can cause a particular *unsafe action* and is triggered by particular combinations of *performance-shaping* factors and *plant conditions*. Error mechanisms are often not inherently bad behaviors, but represent mechanisms by which people often efficiently perform skilled work. However, in the wrong context, these mechanisms may lead to inappropriate human actions that have unsafe consequences.

Expectation Bias: The tendency for people to give more significance to information that confirms their beliefs than to information that contradicts their beliefs.

Frequency Bias: Frequently occurring events are often recalled more easily than scarce events. This can lead to a tendency in people to interpret in-coming information about an event in terms of events that occur frequently, rather than infrequently occurring or unlikely events.

Fixation Error: A failure to appropriately revise the assessment of a situation as new evidence is introduced.

Human Error: In the PRA community, the term 'human error' has often been used to refer to human-caused failures of a system or component. However, in the behavioral sciences, the same term is often used to describe the underlying psychological failures that may cause the human action that fails the equipment. Therefore, in ATHEANA, the term 'human error' is only used in a very general way, with the terms *human failure event*, *unsafe action*, and *error mechanism* being used to describe more specific aspects of human errors.

Human Failure Event (HFE): A basic event that is modeled in the logic models of a PRA (event and fault trees), and that represents a failure of a function, system, or component that is the result of one or more *unsafe actions*. A human failure event reflects the PRA systems' modeling perspective.

Information Processing Model: A general description of the range of human cognitive activities required to respond to abnormal or emergency conditions. The model used in ATHEANA considers actions in response to abnormalities as involving four steps (1) monitoring/detection, (2) situation assessment, (3) response planning, and (4) response implementation.

Mental Model: Mental representations that integrate a person's understanding of how systems and plants work. A mental model enables a person to mentally simulate plant and system performance in order to predict or anticipate plant and equipment behavior.

Monitoring/Detection: The activities involved in extracting information from the environment. Monitoring is checking the state of the plant to determine whether the systems are operating correctly. Detection, in this context, refers to the operator becoming aware that an abnormality exists.

Performance Shaping Factors (PSFs): A set of influences on the performance of an operating crew resulting from the human-related characteristics of the plant, the crew, and the individual operators. The characteristics include procedures, training, and human-factors aspects of the displays and control facilities of the plant.

Plant Conditions: The plant state defined by combinations of its physical properties and equipment conditions, including the measurement of parameters.

Polarization of Thinking: The tendency to attribute events to one global cause instead of a combination of causes.

Primacy Bias/Effects: The tendency in people to give more significance to the data they first see (and may draw conclusions from) than to later data. When judgments or decisions are required, initial information is sometimes more easily recalled than later occurring information.

Probabilistic Risk Assessment/Analysis (PRA): PRA of a nuclear power plant is an analytical process that quantifies the potential risk associated with the design, operation, and maintenance of a plant to the health and safety of the public.

PRA Model: The PRA model is a logic model which generally consist of event trees, fault trees and other analytical tools and is constructed to identify the scenarios that lead to unacceptable plant accident conditions, such as core damage. The model is used to estimate the frequencies of the scenarios by converting the logic model into a probability model. To achieve this aim, estimates must be obtained for the probabilities of each event in the model, including HFEs.

Recency Bias/Effects: Events that happened recently are recalled more easily than events that occurred a long time ago. In attempting to understand in-coming information about an event, people tend to interpret the information in terms of events that have happened recently, rather than relevant events that occurred in the more distant past.

Representativeness Heuristic: The tendency to misinterpret an event because it resembles a "classic event" which was important in past experience or training, or because there is a high degree of similarity between the past event and the evidence examined so far.

Response Implementation: Taking the specific control actions required to perform a task, in accordance with *response planning*. Response implementation may involve taking discreet actions (e.g., flipping a switch) or it may involve continuous control activity (e.g., controlling the steam generator level). It may be performed by a single person, or it may require communication and coordination among multiple individuals.

Response Planning: Deciding on a course of action, given a particular *situation model*. In general, response planning involves identifying plant-state goals, generating one or more alternative response plans, evaluating the response plans, and selecting the response plan that best meets the goals identified.

Rules: Rules are the guidance operators follow in carrying out activities in the plant. Rules can be either formal or informal in nature. *Formal rules* are specific written instructions and requirements provided to operators and authorized for use by plant management. *Informal rules* sources include training programs, discussions among operators, experience, and past practices.

Salience Bias: The tendency to give closer attention or to weight more heavily information or indications that are more prominent, (e.g., the most visible, the loudest, or the most "compelling" instrument displays.)

Satisfying: The tendency in people (under some circumstances) to stop looking for a solution when an acceptable, but not necessarily optimal one, is found.

Scenario Definition: PRA *scenario definitions* provide the minimum descriptions of plant state required to develop the PRA model and define appropriate HFEs. Examples of scenario definition elements include the initiating event, operating mode, decay heat level (for shutdown PRAs), and function/system/component status or configuration. The level of detail to which scenarios are defined can vary and include the functional level, system level, and component state level.

Simplifying: People tend to disregard complex aspects of data, e.g., interaction effects, and give more significance to aspects of the data they understand. This is analogous to searching for a lost item under the lamppost because that is where the light is.

Situation Assessment: Situation assessment involves developing and updating a mental representation of the factors known, or thought to be affecting the plant state, at a given point in time. The mental representation resulting from situation assessment is referred to as a situation model.

Situation Model: A mental representation of the current plant condition, and the factors thought to be affecting the plant state resulting from the operators' situation assessment. The situation model is created by an interpretation of operational data in light of the operator's mental model. (An operator's situation model is usually updated constantly as new information is received; failure to update a situation model to incorporate new information is an error mechanism).

Tunnel Vision: The tendency in people to concentrate only on the information that is related to their prevailing hypothesis, neglecting other important information

Unsafe Action (UA): Actions inappropriately taken, or not taken when needed, by plant personnel that result in a degraded plant safety condition.

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

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

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

NUREG-1624, Rev. 1

2. TITLE AND SUBTITLE

Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)

3. DATE REPORT PUBLISHED

MONTH	YEAR
May	2000

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

6. TYPE OF REPORT

Technical

7. PERIOD COVERED *(Inclusive Dates)*

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

Division of Risk Analysis & Applications
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, DC 20555-0001

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.)*

Same as above

10. SUPPLEMENTARY NOTES

11. ABSTRACT *(200 words or less)*

This report introduces a next-generation HRA method called "A Technique for Human Event Analysis," (ATHEANA). ATHEANA was developed to address limitations identified in current HRA approaches by: (1) addressing errors of commission and dependencies; (2) more realistically representing the human-system interactions that have played important roles in accident response; and (3) integrating advances in psychology with engineering, human factors, and PRA disciplines.

This report is the step-by-step guidebook for applying the method. It describes how to:

1. select and organize the ATHEANA team,
2. perform and control the structured search processes for human failure events and unsafe acts, including a discussion of the reasons that such events occur (i.e., the elements of error-forcing context),
3. use the knowledge encoded in the PRA along with the specialized knowledge and experience of the ATHEANA team to focus the searches on those events and reasons that are most likely to affect the risk, and
4. quantify the error-forcing contexts and probability of each unsafe act, given its context.

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

probabilistic risk assessment
human reliability analysis
severe accident

13. AVAILABILITY STATEMENT

unlimited

14. SECURITY CLASSIFICATION

(This Page)

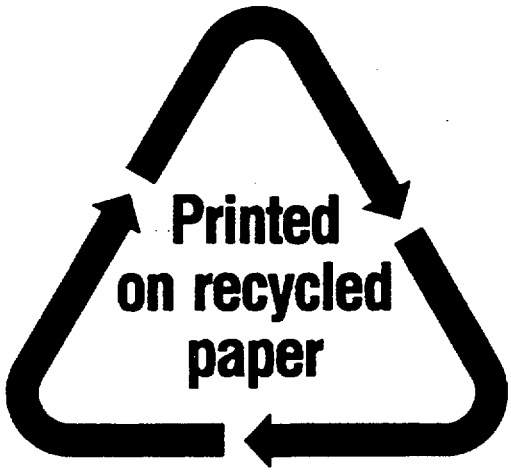
unclassified

(This Report)

unclassified

15. NUMBER OF PAGES

16. PRICE



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

1975 25 years 2000

SPECIAL STANDARD MAIL
POSTAGE AND FEES PAID
USNRC
PERMIT NO. G-67