

**SIGNIFICANT EVENT RESPONSE TEAM  
REPORT NO. 92 - 05  
DECEMBER 29, 1992**

**SALEM UNIT 2  
CONTROL ROOM OVERHEAD ANNUNCIATOR  
LOCK - UP OF DECEMBER 13, 1992**

H/S 2  
H/S 1

December 29, 1992

To the General Manager - Salem Operations

SALEM UNIT 2 - CONTROL ROOM OVERHEAD ANNUNCIATOR LOCK-UP, 12/13/92

SIGNIFICANT EVENT RESPONSE TEAM REPORT

At your request, a **Significant Event Response Team (SERT)** was convened at 23:00 hours on December 14, 1992, to investigate and report on the captioned event.

On December 13, 1992, at 21:22 hours, the Nuclear Control Room Operator (NCO) for Salem Unit 2 received an alarm on the Auxiliary Alarm System (AAS) recording the restoration of the Chilled Water Expansion Tank Level Low to Normal. He then realized the Overhead Annunciator (OHA) for the AAS typewriter had never alarmed, and the clock on the CRT, which displays alarms received by the OHA System, had stopped updating at 19:46 hours. The NCO determined that the OHA System was not functioning, and at 21:23 hours, he reset SER-B and SER-A in the Beta annunciator cabinet located in the Equipment Room. This action restored the functionality of the OHA System.

The SERT charter, as defined by the GMSO, was:

- 1) Independently determine the root cause of the event
- 2) Assess ECG classification and reportability
- 3) Determine if procedures were adequate and followed
- 4) Assess adequacy and design of the OHA System
- 5) Determine corrective actions

The SERT consisted of:

Craig Lambert	Nuclear Engineering and Project Services	Manager
Dan Eskesen	Salem - Operations	Member
Lou Miceli	Salem - Technical	Member
Ken Moore	Salem - Onsite Safety Review	Member
Scott Ward	Salem - Station Quality Assurance	Member
Mike Reese	Nuclear Training Center	Member
Wayne Choromanski	Reliability and Assessment	Member
Lyle Mayer	Nuclear Electrical Engineering	Member
Dennis Connell	Salem - GM Staff	Member

The information in this report is based on our investigation which concluded on December 24, 1992. The team was in operation for 10 days and involved approximately 800 man-hours of work.

Section	Page
I. BACKGROUND INFORMATION	4
II. SYSTEM DESCRIPTION AND LICENSING BASIS	4
III. EVENT CHRONOLOGY	5
IV. EXPLANATION OF EQUIPMENT FAILURES	7
V. SAFETY SIGNIFICANCE OF THE FAILURE OF THE ANNUNCIATOR SYSTEM	7
VI. ASSESSMENT OF EVENT CLASSIFICATION GUIDE (ECG) CLASSIFICATION, IMPLEMENTATION AND REPORTABILITY	8
VII. ASSESSMENT OF PERSONNEL PERFORMANCE	9
VIII. ANALYSIS OF FAILURE DETECTION OPPORTUNITIES	12
IX. ASSESSMENT OF ADEQUACY AND IMPLEMENTATION OF PROCEDURES	14
X. TRAINING	16
XI. REVIEW AND ASSESSMENT OF NEW DESIGN	18
XII. REVIEW OF INDUSTRY EXPERIENCE	20
XIII. ROOT CAUSE ANALYSIS	21
XIV. GENERIC CONSIDERATIONS	22
XV. RECOMMENDATIONS	23
Attachment 1	SIMPLIFIED SYSTEM BLOCK DIAGRAM
Attachment 2	DETAILED SEQUENCE OF EVENTS
Attachment 3	EVENT AND CAUSAL FACTOR FLOW CHART



## I.

BACKGROUND INFORMATION

Modifications were performed to Salem Unit 1 and 2 control consoles and annunciator systems to correct Human Engineering Deficiencies in accordance with NUREG 0700, Guidelines for Control Room Design Reviews. The OHA electronics were modified to replace the existing relay/logic system with a microprocessor based system provided by Beta Products Division of Hathaway Industries. The alarm window displays were re-arranged, relabelled and system reflash capability was modified. On the control console, a CRT with keypad controls and new pushbutton/switches were installed.

The modifications to Unit 2 were completed during outage 2R6 and turned over to Operations on March 26, 1992. The modifications to Unit 1 were completed during outage 1R10 and turned over to Operations on June 12, 1992.

## II.

SYSTEM DESCRIPTION AND LICENSING BASIS

## A. System Description

The Control Room OHA System consists of the Betalog 4100, a high performance sequential events recording system, the Betalarm 1500, a microprocessor based serial input distributed annunciator system, and a Remote Control Workstation Computer (RCW). The OHA consists of ten (10) overhead boxes with forty eight (48) windows per box. The OHA is a non-safety related system. An annunciator CRT display and keypad are located on the control console to identify alarm points.

There are separate and independent pushbuttons located on the control console which the operator uses to silence, acknowledge and reset the OHA system alarms. ~~A key-operated switch is located on the control console to reset "first-out" indications.~~ A test switch is located on the control console for periodic testing of the system.

The OHA is powered by two independent 115 VAC, 60 Hz supplies.

Attachment 1 provides a simplified block diagram of the system.

## B. Licensing Basis

## 1. Safety Evaluation Report

NRC review of the OHA System prior to issuance of an Operating License concluded that the design and safety classification for this system was acceptable. The Safety Evaluation Report did not discuss specific design details.

## 2. UFSAR

UFSAR Section 7.7.2.10 provides a detailed description of

plant alarm and annunciator systems. The OHA System is classified as a non-safety system. Paragraph four (4) on page 7.7-16 states:

"Since Indication and Alarm Systems are not part of the Plant Protection System, and failures within these systems cannot affect the operation of the Protection System, there is no reason to impose limiting conditions for operation on the Alarm Systems. Alarm Systems cannot be considered as part of a safety related system, since they perform no function in the actuation of safety-related equipment. Limiting conditions for operation are imposed on the Plant Protection Systems and equipment to assure the safe operation of the unit."

Design of this system includes consideration of physical separation and electrical isolation between 1E and non-1E circuits, Seismic II/I, Fire Protection, Appendix R requirements and separate and redundant power supplies. Information needed by the operator to respond to abnormal occurrences has been provided in accordance with Regulatory (Reg.) Guide 1.97.

### III.

#### EVENT CHRONOLOGY

All times provided are derived from the SER-B printout.

On December 12, 1992 OHA A-45 (spare) alarmed and was cleared by resetting both SERs. OHA A-45 subsequently alarmed on December 13, 1992. The Nuclear Shift Supervisor (NSS) directed the NCOs not to clear the alarm as it was considered a nuisance alarm and he planned to notify the System Engineer of the problem the following morning.

Between 18:00 and 18:45 hours on December 13th, the Desk NCO accessed the Beta RCW (Panel 115-1) to obtain information associated with the OHA A-45. The NCO performed several keystroke operations on the Beta System RCW keyboard before returning to the control room. Sometime after the Desk NCO left the RCW, the Console NCO accessed the RCW in an attempt to identify the cause for the OHA A-45.

At 19:46 hours, the Unit 2 Beta System clock on the CRT display, stopped updating. At 19:55 hours, the AAS printed "Chilled Water Expansion Tank Level Low", but the associated OHA, "AUX ALM SYS PRINTER" (A-41) did not alarm. The Desk NCO noticed the printout and then directed an equipment operator to fill the tank.

At 20:08 hours, the NCOs performed a containment pressure vacuum/relief which caused radiation monitors 2R13A and 2R13B to alarm. These channels caused "RADIATION ALARM PROCESS" to alarm on 2RP1. The Desk NCO acknowledged the alarm on 2RP1, but neither NCO realized OHA A-6 "RMS TRBL" had failed to annunciate.

At 21:22 hours, "Chilled Water Expansion Tank Level Low" alarm returned to Normal and printed on the AAS. The NCOs then recognized that OHA A-41 did not annunciate. The Console NCO noticed the clock on the OHA CRT was indicating 19:46 hours and not updating.

At 21:23 hours, an NCO reset SER-B, then SER-A, in the Beta Annunciator Cabinet. After the SERs were reset, four OHAs were received in the control room:

- Annunciator Logic (A-9)
- RMS Trouble (A-6)
- 104 Panel Trouble (C-9)
- AAS Printer (A-41).

The Console NCO verified these OHAs coincided with the CRT and that the CRT clock was updating, and notified the NSS.

At 21:32 hours, the AAS printed "Plant Vent Heat Trace Trouble" and associated OHA A-41 alarms. The operators considered this as confirmation the annunciator system had been restored.

The NSS informed the Senior Nuclear Shift Supervisor (SNSS) who began reviewing the Event Classification Guide (ECG) Section 10 for classification/reportability requirements. At approximately 22:00 hours, the SNSS called the Operating Engineer (OE) and indicated 3 minutes (by Beta System 1 minute) had elapsed between the time the OHA system was discovered to be "locked-up" to the time the system was reset. Therefore, after SNSS and OE discussion of the event and review of ECG Section 10, an Alert and NRC One Hour Notification were not applicable.

Subsequently, the NSS called the System Engineer (SE) and discussed the Beta OHA System. The NSS indicated the on-duty technician was not qualified to work on the system. **Therefore, he requested the SE to come in.**

At approximately 23:30 hours, the SE arrived and performed a number of diagnostic tests on the system. These tests verified that SER-A and B were functioning properly. The SE reset SER-A and B to clear the printer error.

The SE discussed the test results with the NSS and indicated he planned to call the vendor in the morning.

See Attachment 2. "Detailed Sequence of Events"

#### IV. EXPLANATION OF EQUIPMENT FAILURES

The SERT performed a thorough review of system failures and malfunctions from the time the system was installed until the system "locked-up" on December 13, 1992. The details associated with this review are included in the Sequence of Events contained in Attachment 2.

Based on a special test performed by a System Engineer and BETA Products Field Engineer on December 18, 1992, the OHA window A-9 alarmed when the SER-A transferred system control to SER-B. The SER-A circuit board was removed and replaced with the temporary OHA circuit board used during system installation.

On December 19, 1992, the removed SER-A circuit board was tested at BETA Products facilities and it was discovered that when "Ctrl L" is entered twice at the RCW PC keyboard with the RCW in PROCOM PLUS and the "Black Box" is in RCW-A position, the SER "locked-up". That is, when the system saw the PROCOM PLUS command, all SER ports were turned off, stopping CRT clock update and alarming valid overhead windows. Review of Salem Unit 2's RCW PC files revealed a file that was created at 19:47 hours on December 13, 1992.

The SERT has determined that the event was caused by a combination of entering "Ctrl L" twice, with the RCW in PROCOM PLUS and the "Black Box" switch in RCW-A, rather than SER-A. When this occurs, the main controller will stop sending events to any display devices that are connected, and wait indefinitely for commands to be sent from the RCW.

#### V. SAFETY SIGNIFICANCE OF THE FAILURE OF THE ANNUNCIATOR SYSTEM

The UFSAR states that the OHA System is not safety related. System alarms are not part of the plant protection scheme and failures cannot affect protective system operation. Therefore, operation limits are not imposed on the plant. Technical Specifications (Units 1 and 2: 3.3.3.5, REMOTE SHUTDOWN INSTRUMENTATION, and 3.3.3.7, ACCIDENT MONITORING INSTRUMENTATION) and Control Room Evacuation, S1(2)-OP.SO-AB.CR-0001(Q), and Control Room Evacuation Due To Fire In The Control Room, Relay Room, or Ceiling of the 460/230V Switchgear Room, S1(2)-OP.SO-AB.CR-0002(Q) ~~do not contain/refer to any overhead annunciators to provide diagnostics or decision points for safe~~ ~~operation of the~~ units.

It is recognized industry-wide that the risk of a degraded plant condition going undetected increases when a majority of the OHAs are lost or unavailable; therefore, emergency declaration is appropriate. The necessary personnel to provide increased monitoring for continued safe operation of the affected unit(s) is accomplished by activation under the E-Plan implementation for



this type of event.

Clarification to ECG Section 10D or development of another IC/EAL for this section is in order. Consider NUMARC/NESP-007, "Methodology for Development of Emergency Action Levels. This is acceptable to the NRC as an alternative method for the development of EALs. It is the result of an industry-wide effort to standardize criteria for classification of emergencies.

Additionally, NESP-007 recognizes that certain loss of OHA scenarios can occur in which the option of calling extra personnel is given to the SNSS. The determination should be guided by Technical Specification **OPERABILITY** concerns or ability to enter and maintain control of the plant during abnormal or emergency procedure operations.

Consideration may be given to the system reliability perspective as well. If the system is unreliable, excessive emergency declarations will occur. This is highly undesirable! Therefore, the system needs adequate reliability/redundancy, without unreasonable expense, to provide that assurance.

Since the OHA System is utilized to recognize abnormal conditions, the UFSAR needs to adequately describe its failure modes, as well as a description of its workings. An electric power loss to the system is described in the proposed FSAR change; however, system ground, computer logic and OHA/MCR Console CRT combination failures are not.

#### VI. ASSESSMENT OF EVENT CLASSIFICATION GUIDE (ECG) CLASSIFICATION, IMPLEMENTATION AND REPORTABILITY

Initial event analysis and classification was prompt and correct. The OHA loss event was classified according to NUREG 0654 Rev. 1. It specifies that emergency declaration is timed from discovery of the condition by the operators. During the OHA loss of December 13, 1992, operators recognized the event and corrected the cause prior to exceeding the 15 minute limit of ECG Section 10B.

SERT concurs with the determination made at the time of the event by the SNSS and OE that an ALERT Declaration was not necessary.

Although classification under the ALERT class is not considered necessary for this occurrence, SERT believes for future events of this type, a courtesy call be made to the Emergency Notification Center informing them of the event.

As discussed previously, the SNSS and OE reviewed ECG Section 10 for Reportability. Section 10 D. requires a one hour report should there be a major loss of emergency assessment capability, specifically loss of "Other Control Room indications or plant monitors necessary for accident assessment". The Annunciator System is not described as Accident Monitoring Instrumentation per

**Technical Specification 3.3.3.7.**

SERT concurs with the position taken by the SNSS and OE on the evening of the event.

At approximately 09:00 hours on December 14, 1992, the event was discussed with one of the Salem Resident NRC Inspectors. After details of the event were known and cause was still under investigation, it was determined by PSE&G Management that a non-emergency declaration was the prudent approach to take.

**VII.****ASSESSMENT OF PERSONNEL PERFORMANCE**

Operator actions and suitability of the response to this event have been determined by reviewing narrative and plant logs, appropriate plant normal, alarm response, abnormal and emergency procedures along with interviewing involved operators, their supervisors and management personnel.

**A. LICENSED OPERATORS:****1. NCO-Console:**

The Console NCO did not notice the loss of OHAs until the AAS Chilled Water Expansion Level Low alarm returned to Normal. Functional capability was lost for approximately 90 minutes. Three alarm conditions (two AAS alarms and one 2RP1 RMS alarm) were actuated over a 90 minute period. All could have given the NCO indication that the OHAs were not operating correctly. Factors that may have affected the identification of the OHA loss could be attributed to the day and shift, Sunday 15:15-23:15. Also, relief for mealtime occurred at or about the time when the alarms were missed.

The above conditions reinforce the need for increased awareness to corroborating indications and thorough temporary relief turnovers during reduced activity times in the Control Room.

Upon recognizing the BETA system CRT not updating, the Console NCO made a brief statement about the BETA System CRT condition to the Desk NCO, then went to reset the BETA SERs according to an Operations Department Information Directive (ID) on the system. The NCO did not know what the condition of the computer system was, but believed that the reset process would correct the condition. Upon resetting, the OHA system seemed to function correctly.

Although the Console NCO did not perform an OHA test, he continued to monitor/compare subsequent OHAs with diverse corresponding Control Room indications to insure operation of the system.

Based on stated information, normal watchstanding activities require increased awareness. Actions to reset the system and follow up monitoring were considered prudent.

2. NCO-Desk:

At approximately 18:00 hours, an attempt was made to access the BETA RCW to identify the cause of A-45. Access to the computer system for historical data printout was attempted utilizing operating procedure S2.OP-SO.ANN-0001(Q). For reasons unknown, the NCO did not place the "Black Box" switch in the proper position, as directed by the procedure. Using computer prompts, several access attempts were made. Upon arriving at a password protected option, several different passwords were tried, all of which were unsuccessful. Password use by operators is not required for operator functions and was not authorized by the procedure. Termination was attempted due to "not feeling comfortable", and the NCO was unsuccessful in gaining the desired information.

Had the NCO been successful in gaining entry with a password, the software integrity could have been compromised.

With the exception of password usage, operations performed at the BETA RCW were under directions of a procedure and computer prompts were not supposed to result in the condition that occurred. *res  
for*

3. Generic:

These items are applicable to Console and Desk NCOs.

- a. The NCOs are responsible for continuous plant monitoring from the Control Room. Close monitoring of auxiliary indications, charts, computer printouts, etc. can assist in determining loss of primary indications/alarms.
- b. Control Room Narrative Logs are the responsibility of the NCO. Both NCOs were aware of the significance of the loss of most or all OHA's. The events leading up to and details of events during the time when the OHA's were not functional need to be detailed in the narrative.

4. NSS:

The NSS, when apprised by the NCO, of the problem associated with the OHA System, notified the Senior Nuclear Shift Supervisor (SNSS) in a timely manner and confirmed that the system appeared to be functioning properly. The NSS participated in the review of the ECG for applicability in his capacity as the Shift Technical Advisor (STA). *do  
this  
cont*

5. SNSS:

Upon being informed of the condition, ECG Section 10 was consulted. The SNSS and NSS/STA determined that entry into any emergency classification was not appropriate.

The SNSS then telephoned the OE, and discussed the ECG Section 10. The OE concurred with the decision not to declare an emergency condition nor make the one hour notification.

Based on the time of discovery and correction of the condition, it was appropriate not to enter into any emergency classification/reportability.

The SNSS contacted the System Engineer to discuss the event and determine if any further actions related to system functionality were required.

Contacting the System Engineer was considered prudent action.

6. OE on call:

After discussing the situation with the SNSS, the OE concurred with the SNSS decision not to declare an ALERT or make one hour notification at that time. Instructions were given to the SNSS to call back if the SE determined the OHA system incapable of carrying out its designed functions.

With the information available to the OE, the decision on the Loss of Overhead Annunciators, was appropriate.

B. NON-LICENSED OPERATOR:

Not Applicable

C. SHIFT CONTROLS (I&C) TECHNICIAN:

Not applicable - the Shift Controls (I&C) Technician was not qualified on the BETA System; no action, no involvement.

D. ENGINEER:

The System Engineer responded promptly upon learning the Shift Controls (I&C) Technician was not qualified on the system.

His actions appeared to be correct for the information and indications available to him upon arrival on site.



# VIII. ANALYSIS OF FAILURE DETECTION OPPORTUNITIES

During the period of SER-A failure (19:46 to 21:23 hours), events occurred that might have afforded opportunities for detection of the SER-A "lock-up" which resulted in the failure of the control room CRT to update, and the failure of the OHA windows to indicate changing plant status/condition.

These opportunities are listed below in the Order of Occurrence and are further discussed by Order of Potential for Detection.

## A. Order of Occurrence

	<u>Time</u>	<u>Source</u>	<u>Parameter</u>	<u>Condition</u>
1.	19:46*	2CC1 CRT	CRT Time display	Fails to update time
2.	19:55	AAS Print	Chilled Water Expansion Tank Level Low - Alarm	OHA A-41 does not annunciate for AAS print
3.	20:08	2RP1 RMS PNL	Radiation Alarm Process	OHA A-6 does not annunciate for 2R13A/B
4.	21:22	AAS Print	Chilled Water Expansion Tank Level Low - Normal	OHA A-41 does not annunciate for AAS print

\* Condition remains throughout period of failure

## B. Order of Potential for Detection

EVENT of HIGHEST POTENTIAL	<p>At 20:08, Radiation monitors 2R13A and B alarmed upon the initiation of containment pressure relief. This was expected and previously experienced. The 2R13s entering alarm caused 2RP1 RMS Panel "RADIATION ALARM PROCESS" window to light. The alarm on 2RP1 RMS Panel should have driven OHA A-6 "RMS TROUBLE" to annunciate. However, since the SER-A was "locked-up" this did not occur.</p> <p>In preparation for performing the containment pressure relief the Desk NCO went to the RMS Panel on 2RP1 and stood by while the Console NCO stroked the pressure/vacuum relief valves open. As the valves stroked open the 2R13 A and B Radiation Monitors entered alarm, the Desk NCO immediately acknowledged the RMS Panel alarm (approximately 1 second elapsed from alarm to acknowledgment) and both the Desk and Console NCOs failed to recognize that the OHA system did not annunciate the alarm condition.</p>
-------------------------------------	--

This opportunity had the highest potential for detection since

both NCOs were aware of the condition, as it occurred, which should have caused an OHA alarm. The operators may have been desensitized to this alarm, in that this condition has existed since November 23, 1992 (containment pressure reliefs are performed approximately once per shift).

The next two events, Chilled Water Expansion Tank Level Low Alarm and return to Normal, are similar in probability for detection when the condition exists by itself. Since the operators were expecting the expansion tank alarm to clear upon initiating actions to fill the tank, the return to Normal had a higher probability of OHA failure detection.

SECOND HIGHEST POTENTIAL	At 21:22, AAS printed return to Normal for Chilled Water Expansion Tank Level Low. This was detected immediately by both NCOs and recognized that the OHA A-41 "AUX ALM SYS PRINTER" did not annunciate. After the AAS printing condition was realized, the 2CC1 CRT was monitored and determined to be not updating since the time display still indicated 19:46.
--------------------------------	--

The Console NCO took prompt action (at 21:23) to re-set the Beta System SER units.

THIRD HIGHEST POTENTIAL	At 19:55, AAS printed Alarm for Chilled Water Expansion Tank Level Low. Without expecting an alarming condition on the AAS and the OHA A-41, the Chilled Water Expansion Tank Level Low Alarm is logged unnoticed on the AAS printer. Detection of the alarm is eventually made during a routine review of the AAS printout. Both NCOs assumed the A-41 OHA had annunciated earlier but could not recall acknowledging and resetting the window.
-------------------------------	--

Normal recognition of AAS events are "forward progression": a parameter enters alarm, begins to print on the AAS printer, initiates OHA A-41, the Console NCO notifies the Desk NCO of the AAS alarm, the Desk NCO evaluates the condition and reports it to the Console NCO, the Console and Desk NCOs determine the appropriate response and take corrective actions. If presented with a condition, they do not instinctively question whether there was an alarm. Instead the progression is picked up at the evaluation phase and continued to corrective action.

During this period the Desk and Console NCOs were relieved one at a time by the NSS. This could have contributed to the unnoticed AAS printout.

LEAST POTENTIAL	The 2CC1 CRT time display failed to update after 19:46 and was a continuous indication of the "lock-up" of SER-A.
--------------------	---

This item, while being of long duration, provided the least probable detection method. This is based on the following

## reasons:

- i. NCOs received no OHA alarms to prompt referencing the CRT for additional information.
- ii. NCOs were not trained to recognize the significance of a failure of the clock to update as an indication of an OHA System failure.

At 21:23 SER-B and SER-A were reset, CRT and OHA responded as previously seen upon SER resets (i.e. time updates occurred on the CRT and the OHA Window lights cycled as described in S2.OP-SO.ANN-0001 step 3.5).

# IX. ASSESSMENT OF ADEQUACY AND IMPLEMENTATION OF PROCEDURES

## A. OPERATIONS

Operations Department had the following procedures in place at the time of the event:

- S2.OP-SO.ANN-0001 "OVERHEAD ANNUNCIATORS OPERATION"
- S2.OP-SO.ANN-0002 "OVERHEAD ANNUNCIATORS GROUND DETECTION"
- OHA A WINDOW ALARM RESPONSE FOR WINDOWS A-1, A-9 AND A-17

Review of the Operations Department OHA responses and ground detection procedures revealed no inadequacies.

Operations Procedure S2.OP-SO.ANN-0001(Q), Rev. 0, "Overhead Annunciators Operation", was utilized during the events leading to the SER-A failure. This procedure is a "Category III" use procedure. Category III procedures allow the completion of the task from memory provided the user is familiar with its use. The operator should refer to the procedure as necessary to perform the job correctly. He is responsible for performing the task in accordance with the procedure.

Areas of concern in the operating procedure were identified during the SERT review for content and use during the event.

1. The procedure purpose stated at step 1.1.E indicates a section of this procedure is the response to an SER failure.

This is incorrect; the section details the operators response to an SER Scanner failure.

2. Step 3.1, description of the "password protected" functions of the RCW, indicate that only "password protected" activities can affect Annunciator System operability.

This is not an accurate assessment as indicated by the event and supporting documentation from the vendor, describing the use of various keystroke combinations, with the six (6) position "Black Box" selected to the RCW "A" or "B" positions.

3. Step 3.5 indicates an SER transfer can be operator initiated at the RCW Computer.

This statement implies the "operators" can force this transfer, which is incorrect and prompts the following concerns:

- The directions to perform this transfer are not provided in the procedure.
- It is not possible to cause a transfer from the RCW Computer. During the investigation the OHA System Engineer indicated it would be necessary to pull the SER card to force a transfer.

4. Section 5.4, RCW operation, directs the operator to "ENSURE the "Black Box" Switch is in the SER-A position".

There is no step in the remainder of the section to return the switch position to RCW-A position. Leaving the switch in the SER-A position will cause the historical buffer to fill and the oldest data to be overwritten as the SER accumulates events beyond 6000.

5. Section 5.4, RCW operation did not provide direction to the operator for all RCW configurations, i.e., the procedure assumes the computer was off at the time the operator enters Section 5.4. The computer was on at the time the operator arrived.

It is SERT's understanding that the RCW computer is always on, and the "Black Box" switch is in RCW-A to allow automatically saving historical data to the hard drive to permit trending by the System Engineers. This may have added confusion to the operator as he attempted to access the system.

(NOTE: Section 5.4 concerns have been addressed. Revision 1 to this procedure has redefined this section and is now used for "Resetting and Testing the OHA System". Steps manipulating the "Black Box" and computer have been removed.)

6. The procedure, as provided, does not contain steps to reset the SERs should the need arise.

During the installation of the Beta OHA System, it was identified that the system "locked-up" while performing an OHA test.

This "lock-up" was addressed in two ways. The immediate response was to issue a letter to the Operations Manager from the Project

Team, describing the occurrence and requesting that operators not perform the test in the manner that led to the "lock-up". The letter also identified that operators on shift were shown how to reset the SERs. The long term response was to make an "EPROM" change which would prevent recurrence of the "lock-up".

Operations response was to issue an Information Directive (ID) with the letter attached. The ID did not include specific instruction on how to perform the SER reset.

During the procedure development the Procedure Upgrade Project (PUP) was not informed by the installation group nor Operations Department of the "lock-up" and need for procedure guidance for SER reset.

7. The procedure, as provided, does not contain guidance for system switch alignment required for operation.
8. The procedure, as provided, does not contain guidance for determination of proper system response/operation.

#### B. MAINTENANCE

No procedures have been developed to date.

#### C. SYSTEM ENGINEERING

No formal procedures have been developed to date

### X.

#### TRAINING

##### A. OPERATOR TRAINING

##### 1. LICENSED OPERATOR:

Salem Licensed Operators received training on the new BETA System in Segment 3 of 1991/92 Licensed Operator Requal Training during the period of January to March 1992. Licensed Operator training was adequate at the time it was conducted. The training consisted of a briefing in the Simulator with demonstration of the functions of the new CRT located on 2CC1. Additionally, the alarm buttons, overhead relocations and alarm horn modifications were demonstrated. Operator training included the operator interface with the system but did not include BETA System hardware and computer systems. Only system components located in the simulator control room were discussed. The RCW was not discussed because it is not planned for installation in the simulator. At that time, a trainee handout, containing a brief description of the system was provided. No further material development nor training has been accomplished since. Operator interface with the system is provided as part of the overall simulator training and in-plant training.



2. NON-LICENSED OPERATOR: Not Applicable

3. ENGINEER:

With the exception of the designated System Engineer, formal training has not been provided to the Station Engineers. The System Engineering Training Core Course does not include Annunciator training, other than system operation demonstration during the simulator portion of their training.

The System Engineer for the BETA system received training during March 1992, while attending the Nuclear Controls (I&C) Technician training.

4. NUCLEAR CONTROLS (I&C) TECHNICIAN:

Initial training was provided by a third party vendor to a group of nine individuals. The group included six Nuclear Controls (I&C) Technicians, two Maintenance Supervisors and the System Engineer. The three-day training course was conducted during the week of March 25, 1992. Training and reference material was provided by a third party vendor.

Although the technician on shift the night of the event was not trained in the Beta System, SERT is not in a position to judge whether additional personnel should be trained or not.

At the time training was conducted, no maintenance procedures had been issued. Training could have been more effective if the Procedure Upgrade Program group generating the procedures had aligned procedure issuance with the scheduled training. Additionally, the training did not contain any of the information on modifications to the system, nor the information contained in Operations Dept ID 92-016, "Unit 2 Control Room OHA". The information, contained in a memo from the DCP Project Manager, was available.

Based on the above information, the training is considered incomplete. A common deficiency appears to be a failure to communicate or transmit advanced installation information to end users in a timely manner, or sometimes, not at all.

The following are SERT recommendations for training that could further reduce the likelihood of future occurrences. For systems significant to plant operation (i.e.: Tech Spec implications, ECG classifications, other identified license conditions, etc.):

- Training prior to release of system/modification for operation.
- Table-top review by the user group prior to turnover of system for operation.

- Walk-thru with several different operators in the "operator mode" of system operation.
- Evaluate methods for improving the interface with the Nuclear Training Center for training requirements associated with the DCP process.

XI.

REVIEW AND ASSESSMENT OF NEW DESIGN

SERT review of SORC approved, Revision 0, Design Change Package (DCP) 2EC-3056 "Phase III Annunciator Modifications" was performed to determine if the DCP for the new OHA System could have contributed to the total loss of Unit 2's Control Room OHA System on December 13, 1992.

The draft DCP was prepared and peer reviewed by an external Architectural Engineer (AE) with inputs from various PSE&G discipline groups, including Salem System Engineering. PSE&G provided final DCP approval.

SERT's assessment of the DCP's engineering design input and review is as follows:

A. ENGINEERING:

This DCP was implemented to upgrade and replace the relay/logic OHA system with a microprocessor based OHA manufactured by BETA Products.

The objective was to utilize as much of the existing system configuration and hardware as possible, such as OHA panels, window boxes, cables, etc. BETA Product's 100 % redundant, OHA System was reconfigured such that a single failure in some components could result in a failure of the entire system. Less than 100 % redundancy was justified and accepted.

SERT's review found that the DCP design analysis did not detail the system software. For example, the BETA Products software was neither validated, or reviewed by the Nuclear Process Computer Group. When the DCP was approved, NUREG CR-4640 "Handbook of Software Quality Assurance Techniques Applicable to the Nuclear Industry" was invoked per Specification S-C-ANN-CDS-0205. Procedure NC.NA-AP.ZZ-0064(Q) "Software Quality Assurance" was issued on November 7, 1990, but was not used for this DCP. Also a new Design/Engineering Administrative Procedure NC.NA-AP.ZZ-0052(Q) "Software Control", which was issued at the same period of DCP issuance, may have brought any potential software problem to light. may info.

System performance requirements, needed to support the original design basis, were not included in the design analysis section

to confirm if the new system met or exceeded the original requirements. For example, BETA's calculated Mean Time Between Failures (MTBF) is 8539 hours (failure of a single optical coupler on one scanner circuit board) or 1.03 failures per year. This predicted failure rate is greater than the actual performance of the original system.

SERT's review of the OHA System design also found that the OHA operation could be impacted by a single failure of any one of the following components:

- Auto RS-232 Switch #1 ID 2XD16481
- Auto RS-232 Switch #2 ID 2XD16349
- Data Cables between Auto RS-232 Switches and Distributed Logic A & B and Control Room CRT respectively.
- SER software/firmware.
- Common Field Input Scanner/optical data link.

The DCP did not provide an alternate means to inform the NCO when the SER locked up and was incapable of alarming.

SERT has concluded that there were precursors during the design and the installation phase, which, had they been pursued, could have precluded this event.

#### B. MODIFICATION AND TESTING:

A review of Section 9.0 Installation, Functional & Operational Testing indicated weaknesses:

- Test instructions were not provided to test system software/firmware in the field.
- Test instructions did not demonstrate SER-A transfer of control to SER-B in all possible scenarios.

#### C. TURNOVER and CLOSEOUT:

Review of this Section indicated weaknesses that may have contributed to the event as follows:

1. DCP Change Documents (CD) did not provide technical information to the Procedure Upgrade Project (PUP) group. PUP developed operating and alarm response procedures based on Beta's operations manual.
2. The DCP Project Team did not provide adequate guidance to mitigate the potential of an SER "lock-up", identification of abnormal OHA operation, and quick OHA recovery because of the following:



- At the time of the initial system "lock-up", the Process Computer Group was not involved in the solution. Because they were not involved, they did not have the opportunity to participate in determining whether there were other failure modes.
- No requirements or technical information on how to perform routine functional tests/checks to demonstrate that the complete system is operational.
- No requirements or technical information for any corrective and preventive maintenance of equipment and software.
- No requirements or technical guidance for abnormal operation of equipment and/or software operations.

## XII.

### REVIEW OF INDUSTRY EXPERIENCE

As part of the SERT investigation, a review and analysis was made to find industry events that may have been precursors to the December 13, 1992 event. This review used the "INPO" data base to recover all "annunciator" event incidents. This search generated 162 items. In addition the response to these documents were reviewed.

Of the 162 items listed, two industry events were found to be similar to the Salem 2 event. The events which were similar were;

1. Significant Event Report 16-92 "Loss of Control Room Annunciators and Plant Monitoring Computer Functions" and OE 5358 "Loss of Non-safety Related Annunciators and Plant Computer"

This Significant Event Report deals with the PALO VERDE 3 event on May 4, 1992. Most control room annunciators became inoperable due to a maintenance work activity. Over several hours, operations staff took corrective actions to reduce power and take compensatory measures including declaring a plant ALERT.

This Significant Event Report was presented to the Salem Operating Experience Feedback (OEF) meeting on September 30, 1992 and reviewed. It was determined that existing programs in place were sufficient (operation procedures, work standards program, etc.).

2. OE 5630 "Control Board Annunciators" and OE 5675

This incident occurred at the Callaway plant on October 16, 1992 causing a partial loss of OHA's. A failed field power supply was replaced under a work request. It was found on October 19, 1992 that the OHA's were out of service for approximately 56 minutes. This condition should have resulted in a plant ALERT on October

17, 1992. An AIT was dispatched to Callaway due to this event.

This item was screened by Reliability & Assessment and sent to the Operations and Technical Managers at Salem and Hope Creek.

The remaining items reviewed include such items as Plant Status's (ps), Design Engineering & Configuration Management (de), Emergency Planner Information Exchange (ep), Fire Protection & Plant Security (fs), Good Practices from INPO (gp), and Hot Line Items (hl). These were reviewed and determined not to be applicable to the event at Salem 2 or were covered in other reviewed documents.

Several plants were contacted to discuss those events that seemed to be similar or of interest to this investigation. No items were found to be identical to the Salem 2 event of December 13, 1992. No information that was reviewed during this investigation would have given any significant information to alert operations personnel that a potential problem could present itself in the form of the type of failure experienced. A search of Nuclear Plant Reliability Database Search (NPRDS) was made and did not yield any failures to Beta equipment used at Salem.

### XIII.

#### ROOT CAUSE ANALYSIS

Attachment 3, Event and Causal Factor Chart provides a summary of significant events, inappropriate actions, causal factors and failed or inadequate barriers associated with this event.

The SERT determined the Root Causes of the Beta OHA System "lock-up" as follows:

**THE SOFTWARE ARCHITECTURE DID NOT CONTAIN ADEQUATE SECURITY TO PREVENT INADVERTENT ACCESS TO SOFTWARE CONTROL FUNCTIONS WHICH PLACED THE SYSTEM IN AN INDEFINITE "LOCK-UP" CONDITION.**

**THE FAILURE TO FOLLOW OPERATING PROCEDURE S2.OP-SO.ANN-0001 (Q) BY NOT PLACING THE "BLACK BOX" SWITCH IN THE SER-A POSITION AND INADVERTENT ENTRY OF "CTRL L" CHARACTERS TWICE, WHERE THE PROCEDURE REQUIRED ENTRY OF "ALT L".**

There were multiple causal factors associated with the Root Causes. The causal factors are as follows:

- A. Design specification S-C-ANN-CDS-0205 "Annunciator System" and Attachment F, "OHA Data Acquisition Data Monitoring" did not adequately specify software, software security and software testing requirements.
- B. The DCP as installed did not meet the Design Specification requirements, specifically the system design was to preclude a catastrophic failure.

- C. The Project Team did not include an E&PB software specialist to provide design guidance, oversight and problem resolution.
- D. The DCP did not adequately address procedure development and/or changes.
- E. Lack of a questioning attitude and insufficient follow-up by the Project Team related to the early system failures during installation.
- F. Inadequate knowledge of the Beta System by users of the system.
- G. The Operators did not receive training on some critical aspects of the system.
- H. The OHA System procedure, S2.OP-SO.ANN-0001(Q), contained incomplete requirements.
- I. The Operators were given misleading information relative to operating the RCW computer (operators were told they couldn't do anything wrong to the computer).

#### XIV.

#### GENERIC CONSIDERATIONS

- A. Proper Training Department Representation on the Project Team.

The Training Department Representative assigned to the project team was not from the simulator group. This oversight prevented the Project Team comments from reaching the simulator group in a timely manner.

- B. Mean Time Between Failure Report

Beta supplied an evaluation of the mean time between failure report (MTBF), which indicates that a "MTBF of 8539 hours can be expected for a "soft" failure of the system due to, in all probability, the failure of one optical coupler or one scanner circuit board. Such a failure is often identified as a "graceful degradation".

This failure rate is approximately equal to one failure per year per unit. Project teams need to be more cognizant of equipment failure rates and their potential for impacts to station equipment.

- C. Timely Revisions to Simulator

The design process requires that the training department be

notified that modifications may be necessary to the simulator. It has been indicated that up to one year could expire until the modification is upgraded to the simulator.

## XV.

RECOMMENDATIONS

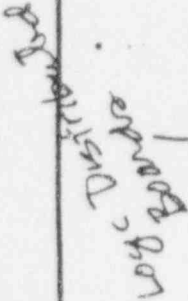
- A. Add an independent circuit/component that monitors OHA operation without using the existing hardware and software and provide a failure alarm in the Control Room.
- B. Add an independent Verification Board that will periodically provide an input to spare field input terminals via a solid state relay and timing circuit for each window box group. The Verification Board would initiate and hold an alarm condition to allow sufficient time for the Console NCO to silence and acknowledge the spare window. Then the Verification Board would clear the alarm condition so the Console NCO can reset the spare window.
- C. Revise Operating Procedure S2.OP-SO.ANN-0001(Q) to provide instructions that describe possible System fault identification, and how the NCO can reset the SERs.
- D. Prepare and issue OHA System Preventive Maintenance and Corrective Maintenance procedures.
- E. Develop an OHA design change to provide 100 % OHA System redundancy.
- F. Clarify ECG Section 10D or develop another IC/EAL for this section.
- G. Provide multiple copies of current 10CFR to the Control Room area for reference.
- H. Review Hope Creek ECG/E-Plan Section 10 ICs and EALs as a result of the Salem OHA loss event.
- I. Revise UFSAR Change Notice for DCP 2EC-3056/PKG1, CD.I582 as follows:
  1. Paragraph 3 and 5 on page 7.7-17 of the change was not changed to reflect the new system configuration for the Beta OHA system.
  2. In paragraph 3, "A contact change of state or change in voltage level indicates an alarm condition until it returns to its normal condition." In fact, the contact is momentary pulsed up in the "make" state and seals in the alarm state, and the pulse down to "break" the condition.
  3. Update the UFSAR to address failure mechanisms that are

inherent to a microprocessor based system.

- J. Reinforce that contract personnel are not authorized to approve UFSAR Change Notices (for the responsible Department Manager).
- K. Have the responsible department manager approve the above UFSAR Change Notice revisions for DCP 2EC-3056/PKG1, CD.I582.
- L. Reinforce the need to maintain complete and detailed control room narratives.
- M. Proceduralize System Engineer manipulation of RCW computer where functions can affect the operability of the OHA System.
- N. For systems significant to plant operation (i.e.: Tech Spec implications, ECG classifications, other identified license conditions, etc.) provide training as follows:
  - 1. Training prior to release of system/modification for operation;
  - 2. Provide walk-thru with operators in system operation.
- O. Evaluate methods for improving the interface with the Nuclear Training Center for training requirements associated with the DCP process.
- P. Establish Software Specialty Review in the DCP process for DCP's involving software and firmware modification/installation.
- Q. Perform test of "CTRL L" "CTRL L" on the Beta System during refueling 2R7 to verify results are as stated in the vendor supplied evaluation.

  
 Craig Lambert  
 SERT Manager





SERT Report 92-05  
Attachment 2

DETAILED SEQUENCE OF EVENTS

- 10/16/90 - Bid Design Specification issued, Rev. 0.
- 12/12/90 - Bid Specification evaluated and awarded to Beta Products.
- 5/3/91 - ECG revised to clarify the Emergency Action Level for an Alert or Site Area Emergency when Control Room Annunciators are lost.
- 8/13/91 - Unit 2 Bid Specification, Rev. 1.
- 10/7/91 - Unit 2 Beta System Acceptance Test completed at the Beta Facility.
- 10/31/91 - DCP 2EC-3056, "Beta Annunciator System" (SER-4100) reviewed and approved by SORC.
- 11/1/91 - Station Manager approves DCP 2EC-3056.
- 12/31/91 - Licensed Operators complete training on ECG revision during Segment II.
- 1/92 - 3/92 - Unit 2 Beta Annunciator System (SER-4100) DCP installed and tested during 2R6.
- 2/23/92 - Unit 2 operators inadvertently "lock-up" the SER Computer and extinguish all alarms in window boxes "G", "H", "J", and "K" by activating OHA lamp test switch and depressing the OHA "silence" and "acknowledge" pushbuttons on the control console simultaneously during the installation and testing phase. The "lock-up" condition was cleared by depressing the reset buttons on SER Main and Aux controllers which returned the system to operation. Operators on shift at the time were instructed on the method of resetting the SER Main and Aux Controllers.
- The System Engineer calls Kewaunee Station to learn they have a 100% redundant system and use interlock wiring change to RSA switches.
- System Engineer requests project team to rewire Salem's OHA RSA switches.
- System Engineer informs Control Room Modification Group Project Team since there is only one data line between SER-A & B and distributor boards a single data line (RS232) failure (P1), then OHA is not functional.

SERT Report 92-05  
Attachment 2

- 2/24/92
- Operators inform Control Room Modification Group that 2 alarms in window box "A" were illuminated without cause. SER was reset, but several alarms in window box "A", "B", "E", and "F" remained illuminated. Found a "Checksum Error" on boards 3 and 9. Boards reset by removing then reinstalling associated fuses F1 and F2 on each board, followed by an SER reset returned the system to operation.
- 2/25/92
- Letter from Control Room Modification Group Project Manager to Operations Manager recommending the operators refrain from depressing both pushbuttons simultaneously until a software change (EPROM) can be made.
- 3/5/92
- Operations informs Control Room Modification Group that 9 alarms in "F" window are illuminated without cause. "Checksum error" found on board 18. Board reset by removing and reinstalling associated fuses F1 and F2, then resetting the SERs, which returned the system to operation.
- 3/8/92
- Operations informs Control Room Modification Group that several windows had not operated properly during an I&C test over the weekend. I & C indicates window F-20 had not responded properly during I&C testing. Beta equipment receiving the alarm input, but gave no response. "Scanner #10 failure", scanner board reset by unplugging and reinstalling cables on scanner board #10 cleared the problem.
  - Operations Manager issues an Information Directive (#92-016) to all operating shifts with the attached 2/25/92 letter from the Control Room Modification Project Manager, to refrain from depressing pushbuttons simultaneously until a software change can be made.
- 3/11/92
- Letter from Project Manager to Beta Products expressing concern of 2/23, 2/24, 3/5, and 3/8 occurrences which had not been detected as a "Logic Failure" on the OHA system. Additionally, he indicates the loss of the OHA System for a period of time would put the station in the "ALERT" status requiring Local, State, and Federal (NRC) notifications.



SERT Report 92-05  
Attachment 2

- 3/17/92 - Operating procedure ANN-1 & ANN-2 issued without information regarding requirements for criteria for functional capability or use of the "reset" pushbutton.
- 3/20/92 - Licensed Operators complete training on the new Unit 2 Beta Annunciator System during Segment III. The training was conducted on the simulator and included movement of the acknowledge pushbuttons and operation of the alarm CRT.
- 3/25/92 - Salem Maintenance Department I&C personnel complete a three-day training program on the new Beta Annunciator System. A System Engineer, 2 I&C Supervisors, and 6 technicians completed the course.
- 3/26/92 - Beta Annunciator System turned over to Operations with a two-page exceptions list which includes EPROM change to preclude system "lock-up" during OHA lamp test.
- 4/9/92 - EPROM change from version 2.07 to 1.11 completed on distributed annunciator boards to preclude system "lock-up" during OHA lamp test using more than one pushbutton.
- EPROM change from version 1.14 to 1.15 on SER-A and B.
- 4/10/92 - Operators report 4 alarms in window box "E" (E-7, 15, 23, 47) illuminated that should not be, but the CRT display updates properly. The cause is attributed to "BLAISE ERROR MESSAGE" per Assistant Project Manager letter to Beta Products dated 4/15/92. However, SMD-IC indicated on WO# 920410120 they replaced logic board "E" and board "8". Found an "ECHO" problem in software and pulled fuses causing the problem to disappear. A satisfactory test was performed by the Test Group.
- 4/16/92 - System Engineer reports the first out windows were not coming up red. He runs tests to clear problem windows, but 2 alarms cleared that should have remained in alarm. He reset SER-A and B and the 2 windows re-alarm. Only had a "BLAISE ERROR MESSAGE". Beta trying to duplicate error problem at Dallas office.
- 5/28/92 - "Checksum Error". Logic board replaced under WO #920528142.

SERT Report 92-05  
Attachment 2

- 5/92 - 6/92 - DCP 1EC-3085, "Beta Annunciator System" design change installed and tested.
- 6/12/92 - Unit 1 Beta Annunciator System turned over to Operations.
- 8/14/92 - OHA "Annun Logic Failure" (A-9) alarms due to "Checksum Error" on board 4. Under WO #920814137 SMD-I&C gives instructions to board 4 to clear error and OHA A-9.
- 10/3/92 - Unit 2 CRT unit found broken. It is replaced by SMD-I&C under WO #920929183.
- 11/23/92 - Unit 2 backdraft damper leaking-by causing containment atmosphere to flow back through vacuum relief unit causing 2R13A to spike. A work request was written (#921123184) on 11/23/92, but the problem continues to cause RMS Trouble OHA to annunciate unnecessarily during containment pressure relief. Containment pressure reliefs are performed approximately once per shift, on average.
- 12/12/92 @ 15:00 - Spare OHA window (A-45) in alarm when swing shift NCOs enter the Unit 2 control room.
- OHA "Lower Section Deviation Above 50% Power" alarms approximately 5,000 times. The cause was attributed to NIS contact chatter.
- @ 20:00 - NCO clears Spare OHA window (A-45) by resetting SERs in equipment room cabinet.
- @ 21:37 - OHA "21B-23B Screen Trouble" (G-15) did not alarm @ 12" dp before 21B CW Pump emergency tripped at 10' dp. However, AAT printed "21B Traveling Screen Diff 10 Feet H2O"
- 12/13/92 - OHA "Lower Section Deviation Above 50% Power" alarms and clears approximately 29,000 times throughout the day attributed to NIS contact chatter.
- @ 01:00 - Spare OHA window (A-45) alarms a second time and the Console NCO acknowledges.
- NSS notified by NCOs of alarming condition.
- NCO clears OHA window (A-45) a second time.
- Spare OHA window (A-45) alarms a third time and Console NCO acknowledges.

SERT Report 92-05  
Attachment 2

- 04:00 - OHA "Condensate Return Tank Level Hi/Low" (G-45) alarmed and lit without supporting CRT display.
- 12:00 - OHA G-45 cleared by operator in field with no CRT support for clearing.
- @ 15:00 - Console NCO informed at turnover the acknowledge and reset OHA pushbuttons didn't work approximately 3 times during the day shift.
  - Console NCO asks NSS if he wants OHA A-45 window cleared.
  - NSS directs NCO not to clear OHA A-45 because he plans to notify the System Engineer of the problem in the morning.
- @ 17:00 - OHA "Lower Section Deviation Above 50% Power" clears the final time.
- @ 18:00 - Beta auto functional test completed SAT
- 18:00 - Desk NCO accesses Beta RCW (Panel 115-1) to obtain information associated with OHA A-45.
- @ 18:18 - First "password" use attempted.
- @ 18:36 - Second "password" use attempted.
- @ 18:38 - "22 ABV Exhaust Fan Loss of 125 VDC" and associated OHA "AAS Printer" (A-41) alarms in the control room.
  - ? - Console NCO accesses RCW in an attempt to identify cause for OHA A-45.
- @ 18:48 - OHA "Condensate Polisher Regeneration System Trouble" (G-44) alarms. This is the last alarm received through the Beta Annunciator System prior to "locking-up".
- @ 19:00 - Beta auto functional test completed SAT
- @ 19:14 - Third "password" use attempted.
- 19:36 - "RCW Error 1" archived three times.

SERT Report 92-05  
Attachment 2

- t=0 min @ 19:46 - Beta Annunciator System clock on Overhead Annunciator Display (CRT) stops timing (i.e., "locks-up") due two CTRL-L characters with PROCOM Plus connected to BPA port (i.e., RCW-A position on switch above RCW computer).
- t=9 min @ 19:55 - AAS prints "Chilled Water EXP. TK. Level Low", but the associated OHA "AAS Printer" (A-41) fails to alarm.
- ? - Desk NCO notices the printout and directs an NEO to fill the tank.
- \* TAMS @ 19:56 - Console NCO exits control room area after being relieved by NSS.
- \* TAMS @ 19:59 - Console NCO returns to control room area (Console NCO outside control area for 3 minutes) and Desk NCO leaves control room area.
- t=20 min @ 20:06 - Desk NCO returns to control room area.
- \* TAMS (Desk NCO outside control room area for 7 minutes)
- t=22 min @ 20:08 - 2R13A & 2R13B alarm setpoint reached during a containment pressure relief causing associated 2RP1 window (Radiation Alarm Process) to alarm. OHA "RMS Trouble" (A-6) fails to alarm.
- Desk operator acknowledges the alarm on 2RP1, but Board Operator doesn't notice OHA "RMS Trouble" (A-6) does not alarm.
- t=96 min @ 21:22 - Chilled Water EXP. TK. Level Low alarm returns to Normal and prints on AAS without associated OHA "AAS Printer" (A-41).
- NCOs notice associated OHA "AAS Printer" (A-41) did not alarm.
- NCOs notice the clock on the Overhead Annunciator Display (CRT) is not updating. It indicates 19:46 hours.
- t=97 min @ 21:23 - NCO manually resets SER-B then SER-A in Beta Annunciator System cabinet in the equipment room.
- OHAs "Annunciator Logic Failure" (A-9), "RMS Trouble" (A-6), "104 Panel Trouble" (C-9), and "AAS Printer" (A-41) alarm after SERs reset.
- Console NCO acknowledges the OHAs.

SERT Report 92-05  
Attachment 2

- t=106min @ 21:32 - NCO verifies the clock on Overhead Annunciator Display (CRT) begins updating.
- NCOs verify AAS printouts coincide with OHA windows.
  - NCOs notify NSS .
  - AAS prints "Plant Vent Ht Tracc Trouble" and associated OHA "AAS Printer" (A-41) alarms, therefore the operators considers this as confirmation the annunciator system has been restored.
  - NSS notifies SNSS
  - SNSS reviews the ECG
- @ 22:00 - SNSS calls Operating Engineer and indicates 3 minutes had elapsed between the time the Beta system was discovered to be "locked-up" to when the system was reset. Therefore, NRC notification was not required.
- NSS calls the SE and discusses the Beta Annunciator System. NSS indicates the on-duty technician is not qualified to work on the system. Therefore, he requests the SE to come in.
- @ 22:05 - Fourth "password" use attempted.
- @ 23:30 - System engineer arrives and talks to NCO leaving control room. NCO asks if his use of RCW PC would cause system lock-up. System engineer states 'no'.
- System Engineer begins performing diagnostic tests on the system.
- @ 23:45 - System engineer cannot log on RCW with password for 20 minutes.
- 12/14/92 @ 00:10 - System engineer down loads RCW PC to floppy disk for the past 4 days.
- @ 00:20 - SE reviews SER-A and B alarm events.
- SE verifies SER-A and B are reading the same alarms using Alarm Summary (AS). Therefore, he concludes SER-A and B are logging the same information.

SERT Report 92-05  
Attachment 2

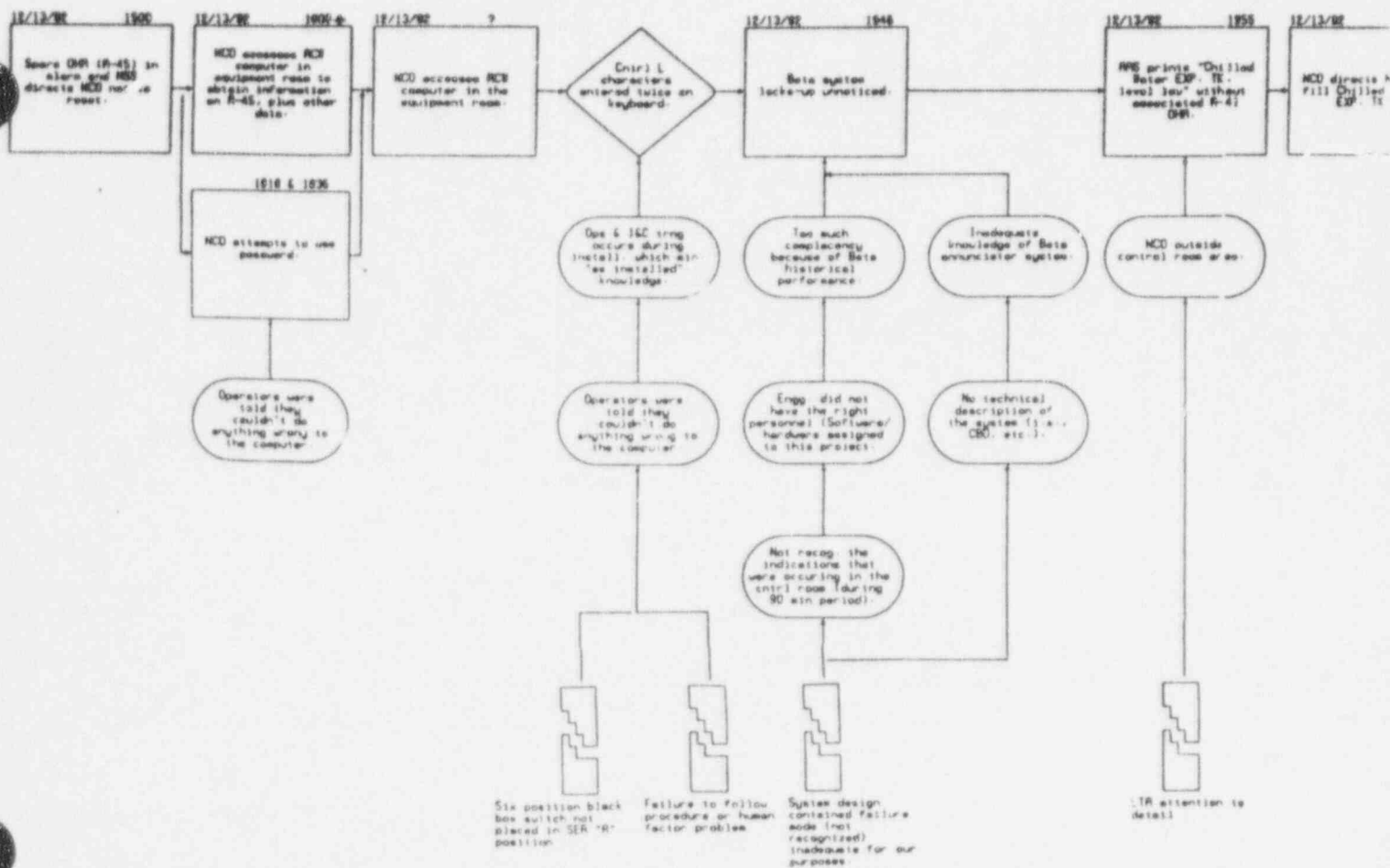
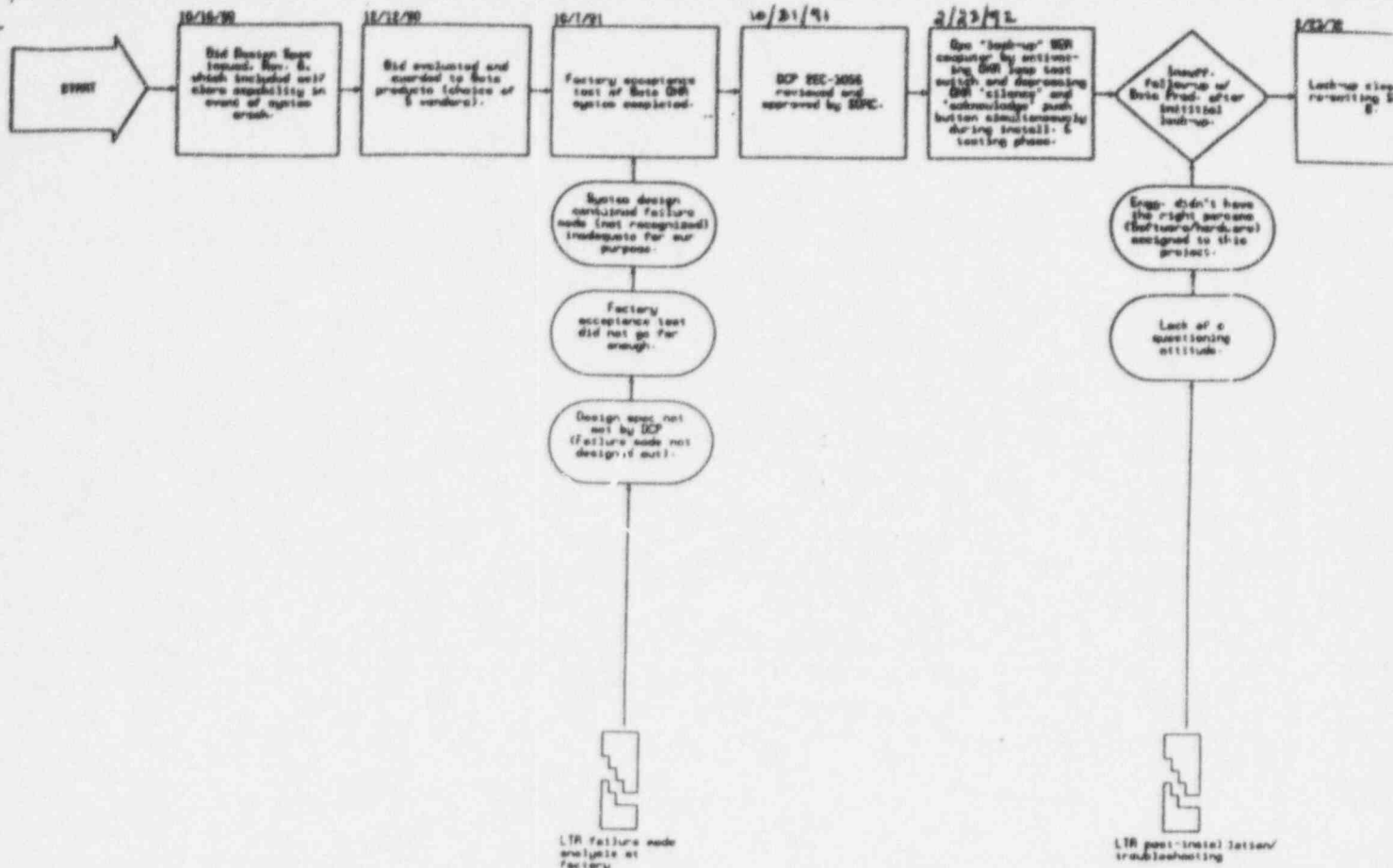
- @ 00:30 - SE uses RCW "PROCOM PLUS" Program and performs SER diagnostics such as Functional Tests (FT), Alarm Summary (AS), Scanner Failures, Port Failures, Point Failures.
- @ 00:35 - At operator panel in the equipment room the SE performs: FT, AS, and selected point statuses. SE prints historical buffer of SER-A for the last 400 events.
- @ 00:40 - SE leaves RCW in PROCOM PLUS because of printer communication problem. RCW can not download from SER-A and B in this mode.
- @ 00:41 - OHA "H2 Purity Lo" alarms, but NCO can't acknowledge for 1 minute. SE repeats diagnostic tests which are SAT.
- @ 00:42 - SE tells NCO to issue WR for H2 purity alarm reset problem.
- @ 01:00 - SE performs "CONFIG" diagnostic program for the logic panels (i.e., overhead window box logic drivers). All logic tests are SAT.
- @ 01:15 - SE verifies: power supply LEDs are illuminated, no ground detection LEDs are illuminated, primary LEDs are lit on auto RS-232 switch, bottom "Normal" illuminated on SER-A and B.
- @ 01:30 - SE returns RCW to RCW program and still finds a printer error.
- @ 01:45 - SE resets SER-A and B in an attempt to clear the printer error, but the printer error remains.
- @ 02:00 - NSS writes an Incident Report (#92-822) indicating the OHA system was effectively disabled for a period of approximately 90 minutes.
  - SE and NSS discuss SE test results. SE states OHA was not operating properly before the 21:23 hours reset. NSS has serious operability concerns.
  - SE said he will call vendor in morning. SE observes AAS and OHA working SAT and returns to his work area to review printouts. SE compares his alarm printouts printed prior to 22:00 hrs. on 12/13 and events coincide SAT.



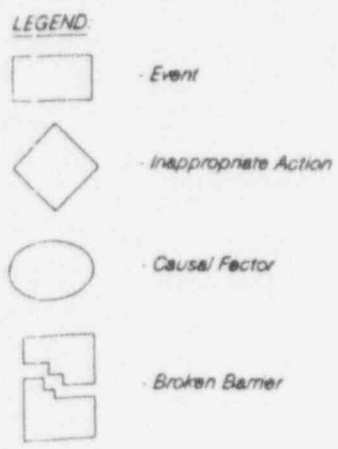
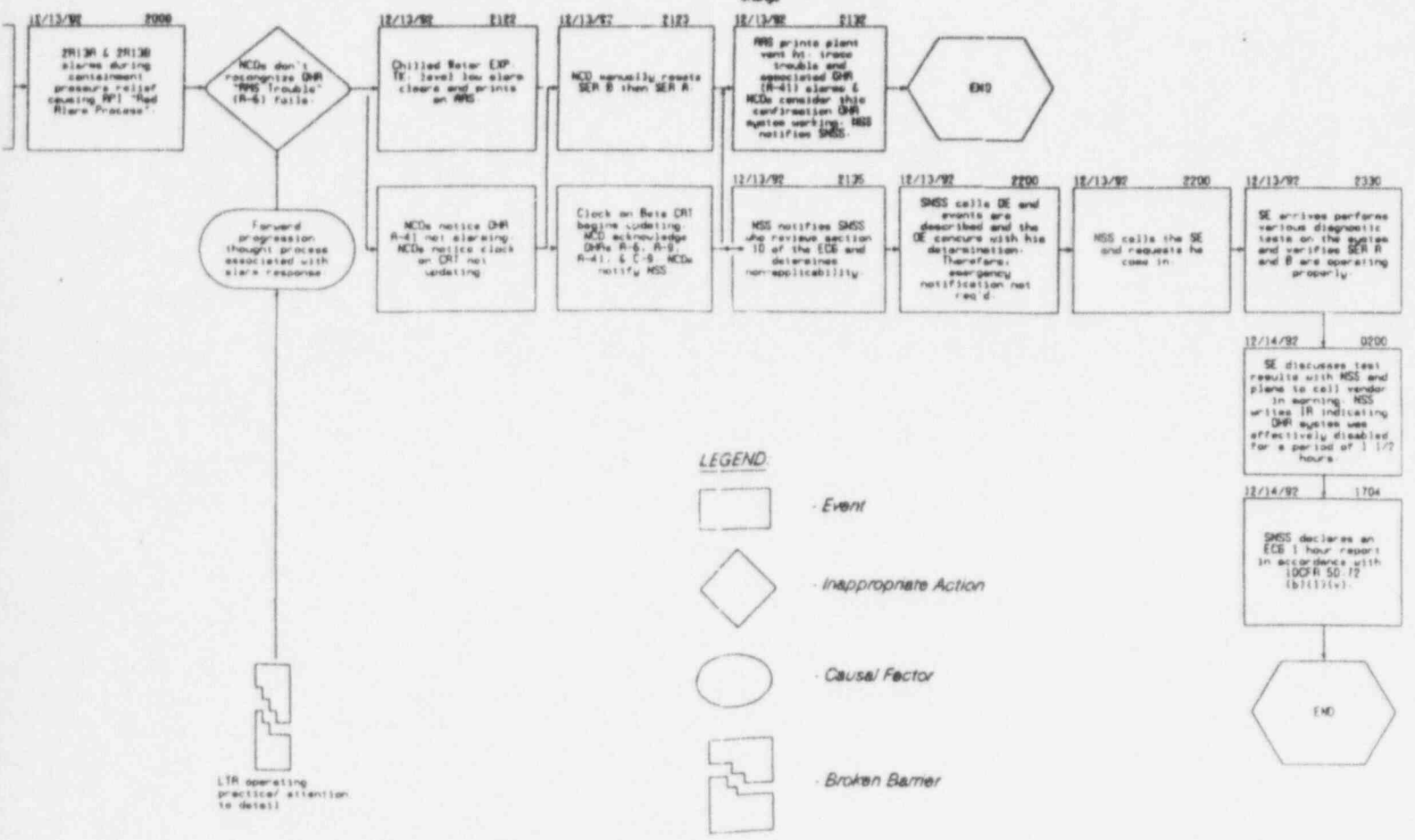
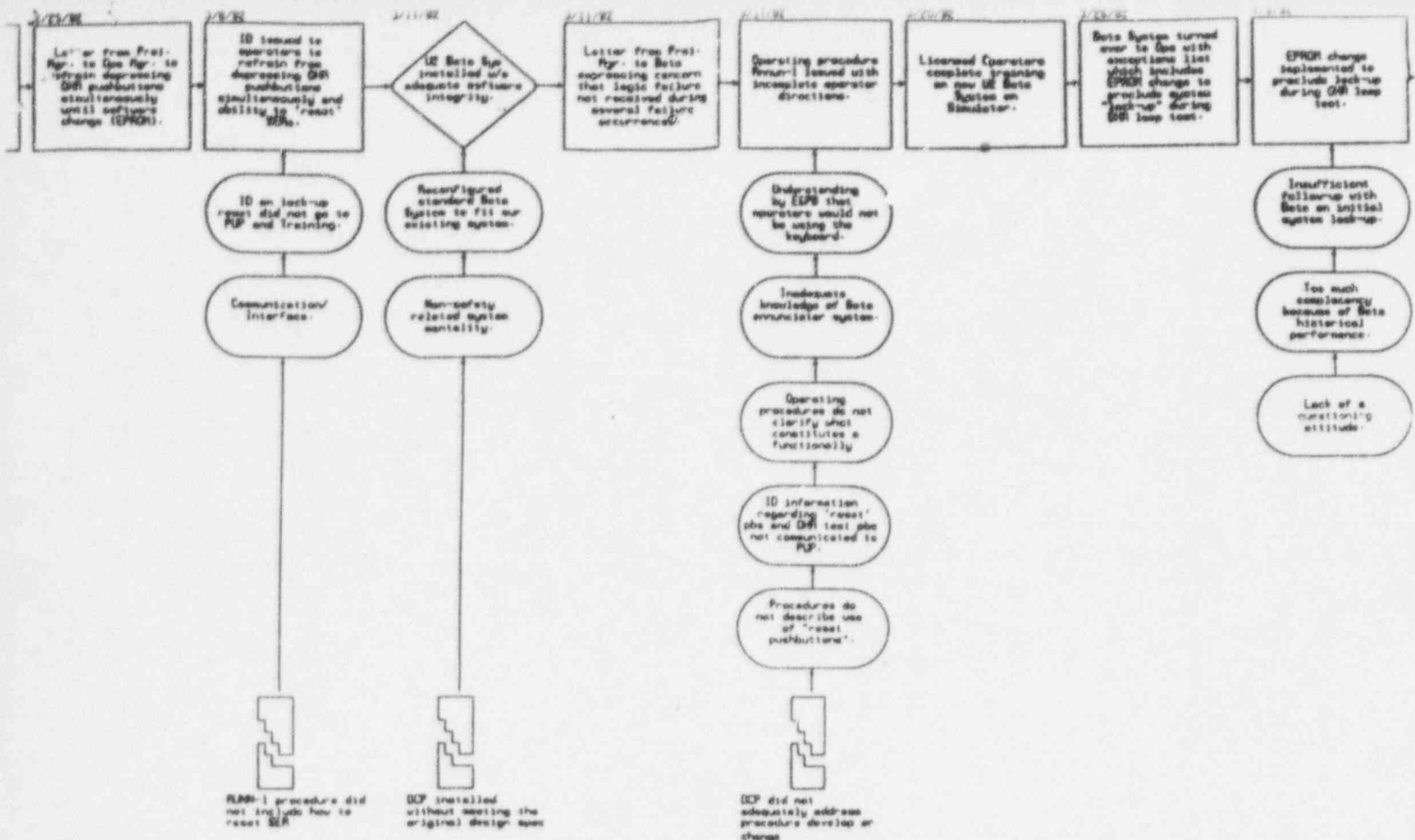
SERT Report 92-05  
Attachment 2

- @ 02:00 - SE review of SER printout did not show AAS Alarms (A-41) at 19:55 and 21:22 on 12/13. No A-9 logic failure on OHA printout. SE aware of clock stop at 19:46 hrs and informs Ops that OHA was not operating from 19:46 until Ops reset system.
- 09:00 - NRC Resident notified of event.
- @ 11:30 - SNSS contacts Emergency Preparedness to discuss ECG.
- @ 17:04 - SNSS declares an ECG 1 hour report in accordance with 10CRF50.72(b)(1)(v).
  - ? - Night Order Book entry made by Operating Engineer to take additional OHA system readings every 15 minutes.
- @ 20:30 - Unit 1 & 2 Operators begin taking readings every 15 minutes on Beta Annunciator System to verify functional capability.
- 12/15/92 @ 11:00 - Incident Report written because the Acknowledge, Silence, and Reset pushbutton was lost.
  - Unit 2 Beta System will not acknowledge, incoming or clear alarms. WO #921215105 written.
- 12/18/92 @ 10:30 - SORC approves a Unit 2 Test procedure for the Beta System.
- 12/18/92 @ 12:00 - Unit 2 Beta Annunciator System Testing commenced. SER-A card removed to be tested in Dallas.
- 12/19/92 @ 23:00 - SORC approves Unit 1 & 2 Justification for Continued Operation.

\* TAMS computer time may deviate by as much as 5 minutes and 53 seconds from the Beta System times as used in this report.







WEST NSAL PSE-93-212



Westinghouse  
Electric Corporation

Energy Systems

Box 356  
Pittsburgh Pennsylvania 15230-0356

June 30, 1993

PSE-93-212

Mr. Dave Perkins, Manager  
Procurement Quality Assurance  
Public Service Electric and Gas Company  
P. O. Box 236  
M/C N-14  
Hancocks Bridge, New Jersey 08038

Public Service Electric and Gas Company  
Salem Units No. 1 and 2  
Inadvertent ECCS Actuation at Power

Dear Mr. Perkins:

The subject Nuclear Safety Advisory Letter is forwarded for your information and use. This letter provides the Westinghouse conclusion regarding 10CFR21 reportability, plant applicability, safety significance and recommended actions.

Westinghouse is unable to evaluate whether deficiencies or failures to comply would create a substantial safety hazard due to insufficient plant application information. The attached information is being provided under the requirements delineated in 10CFR21.21(b) which requires Westinghouse to inform affected customers of this determination.

If you have any questions concerning this Advisory Letter, please let me know.

Very truly yours,

J. R. Gasperini, Manager  
Regional Sales Support

Attachment

*Handwritten notes:*  
H/S  
H/S  
H/S



Westinghouse  
Energy  
Systems  
Business  
Unit

## NUCLEAR SAFETY ADVISORY LETTER



THIS IS A NOTIFICATION OF A RECENTLY IDENTIFIED POTENTIAL SAFETY ISSUE PERTAINING TO BASIC COMPONENTS SUPPLIED BY WESTINGHOUSE. THIS INFORMATION IS BEING PROVIDED TO YOU SO THAT A REVIEW OF THIS ISSUE CAN BE CONDUCTED BY YOU TO DETERMINE IF ANY ACTION IS REQUIRED.

P.O. Box 355, Pittsburgh, PA 15230-0355

Subject: Inadvertent ECCS Actuation at Power	Number: NSAL-93-013
Basic Component: Transient Accident Analysis	Date: June 30, 1993
Plants: See Page 2, Table 1	
Substantial Safety Hazard or Failure to Comply Pursuant to 10 CFR 21.21(a)	Yes <input type="checkbox"/> No <input type="checkbox"/>
Transfer of Information Pursuant to 10 CFR 21.21(b)	Yes <input checked="" type="checkbox"/>
Advisory Information Pursuant to 10 CFR 21.21(c)(2)	Yes <input type="checkbox"/>
Reference:	

### SUMMARY

Westinghouse has discovered that potentially non-conservative assumptions were used in the licensing analysis of the Inadvertent Operation of the ECCS at Power accident. Based on preliminary sensitivity analyses, use of revised assumptions could cause a water solid condition in less than the 10 minutes assumed for operator action time. If the PORVs were blocked, the PSRVs would relieve water and potentially cause the accident to degrade from a Condition II incident to Condition III incident without other incidents occurring independently. Per ANS-051.1/N18.2-1973, a Condition II event cannot generate a more serious event of the Condition III or IV type without other incidents occurring independently.

Westinghouse is unable to determine whether a defect causing a substantial safety hazard or a failure to comply resulting in a substantial safety hazard exists because sufficient plant specific information is not available. Under 10 CFR 21.21(b), if Westinghouse determines that there is insufficient information available to provide the capability to perform an evaluation, then Westinghouse must inform affected licensees of this determination.

Additional information, if required, may be obtained from the originator. Telephone 412-374-4302.

Originator(s):

G. G. Arnett

K. J. Vavrek

H. A. Sepp, Manager  
Strategic Licensing Issues

TABLE 1 PLANT APPLICABILITY LIST

Byron 1 & 2	Almaraz 1 & 2
Braidwood 1 & 2	Doel 1, 2 & 4
Zion 1 & 2	Vandellos
V. C. Summer	Asco 1 & 2
D. C. Cook 1 & 2	Krsko
Shearon Harris	Beznau 1 & 2
W. B. McGuire 1 & 2	Ringhals 2, 3 & 4
Catawba 1 & 2	Tihange 1 & 3
Beaver Valley 1 & 2	Zorita
J. M. Farley 1 & 2	C. N. des Ardennes
Vogtle 1 & 2	C. N. BR3
Seabrook	Kori 3 & 4
Millstone 3	Yonggwong 1 & 2
North Anna 1 & 2	Maansham 1 & 2
Surry 1 & 2	Mihama 2
→ Salem 1 & 2	Ohi 1 & 2 (note 1)
Diablo Canyon 1 & 2	Takahama 1 (note 1)
Wolf Creek	
Callaway	
Sequoyah 1 & 2	
Watts Bar 1 & 2	
Haddam Neck (note 1)	

Notes: 1. Westinghouse is not cognizant of the current ECCS design for these plants.

## TECHNICAL DESCRIPTION

### ISSUE DESCRIPTION

The Inadvertent Actuation of the Emergency Core Cooling System (ECCS) accident (also referred to as the Spurious SI event) is a Condition II incident as defined by ANS-051.1/N18.2-1973, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants." A Condition II incident is defined as a fault of moderate frequency, which, at worst, should result in a reactor shutdown with the plant being capable of returning to operation. A Condition II event cannot generate a more serious event of the Condition III or IV type without other incidents occurring independently.

Standard Review Plan NUREG-0800, Rev. 1, Section 15.5.1, "Inadvertent Operation of ECCS that Increases Reactor Coolant Inventory," states that to meet the requirements of GDC 10, 15, and 26 for incidents of moderate frequency an incident of moderate frequency should not generate a more serious plant condition without other faults occurring independently. To address this, Westinghouse adopted the following criterion:

The pressurizer shall not become water solid as a result of this Condition II transient 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 basis for demonstrating that the pressurizer will not become water solid is to preclude the possibility of discharging primary coolant through the Power Operated Relief Valves (PORVs) and/or the Pressurizer Safety Relief Valves (PSRVs), causing the incident to progress from one of moderate frequency to an infrequent small break LOCA incident. A small break LOCA condition could result from failure of the PSRVs to close after discharging water since the PSRVs were typically not designed for water relief.

Based on a review of the analysis methods used to evaluate this accident, it was discovered that these methods were developed with the primary emphasis on criteria for maintaining RCS pressure below the design value and ensuring that fuel cladding integrity is maintained. These methods did not emphasize the criterion for preventing the pressurizer from becoming water solid within the allowable operator action time. Sensitivity analyses performed for this accident have shown that some analysis assumptions are non-conservative with respect to maximizing the potential for pressurizer filling. Revised analysis assumptions that conservatively consider the potential for pressurizer filling for the Inadvertent Operation of the ECCS at Power accident have been found to have a significant effect on the rate at which the pressurizer water volume increases.

### TECHNICAL EVALUATION

Westinghouse has performed preliminary sensitivity analyses that indicates for some plant specific applications using revised assumptions the pressurizer can become water solid in less than 10 minutes. To conclude that Standard Review Plan NUREG-0800 is met, it must be demonstrated that the pressurizer does not become water-solid in the minimum allowable operator action time, that the PSRVs do not open, or that the PSRVs are capable of successfully closing following water relief. If ECCS flow is not terminated before water is discharged through the PSRVs, it cannot be demonstrated without plant specific PSRV operability assessments that this accident does not lead to a more serious plant condition. Water relief through the PORVs is not a concern, because the PORV block valves can be used to isolate the PORVs if they fail to close. If ECCS flow is not terminated before the pressurizer becomes water solid and water is discharged through the PSRVs, it can not be demonstrated that this accident does not lead to a more serious Condition III LOCA event.



### TECHNICAL EVALUATION (con't)

The analysis for licensing basis assumed maximum ECCS flow which typically includes an additional 5 to 10 percent margin on discharge pressure above the vendor's specified pump performance. The licensing basis analysis assumed that the PORVs, the pressurizer water level control system, the steam dump system and the steam generator PORVs were not available to help mitigate this accident since they are considered to be control grade functions. Also, no credit was taken for letdown since it is isolated following a safety injection signal for those plants which use charging pumps for high head safety injection pumps.

### ASSESSMENT OF SAFETY SIGNIFICANCE

Analyses of the Inadvertent ECCS Actuation at Power accident using revised analysis assumptions with the primary emphasis on conservatively demonstrating acceptability with respect to pressurizer filling have been performed. These analyses show a potential for reaching a water solid condition before the allowable operator action time. Without the appropriate operator action to terminate the ECCS flow prior to reaching a water-solid pressurizer condition, the accident may progress from a Condition II to a more severe Condition III LOCA event as a result of failure of the PSRVs due to water relief through the valves.

X Although Westinghouse previously adopted the conservative criterion of preventing the pressurizer from becoming water solid, the acceptability of water leakage from the RCS for Inadvertent Operation of ECCS Condition II events is supported by NUREG-0800 and ANS-051.1. To meet the applicable Condition II criteria, the magnitude of any water relief must not exceed that of the normal makeup systems (which it will not by definition since this is the cause of the water relief) and the ability to orderly shutdown the reactor must be maintained. The latter implies that the RCS must ultimately be isolated. Hence, the PSRVs must either not open or must be capable of closing after release of subcooled water.

### NRC AWARENESS/REPORTING CONSIDERATIONS

Westinghouse is unable to determine if this issue would cause a substantial safety hazard or a failure to comply resulting in a substantial safety hazard because sufficient plant specific information is not available. This information is being transferred to the applicable plants pursuant to 10 CFR 21.21(b). The NRC has not been notified of this issue.

### RECOMMENDED ACTIONS

1. Licensees should first determine if their current licensing basis requires them to analyze the Inadvertent Operation of the ECCS at Power accident. If this accident is not included within their current licensing basis, no additional action is required.
2. Licensees should determine if their Pressurizer Safety Relief Valves are capable of closing following discharge of subcooled water. If the PSRVs were designed or qualified to relieve subcooled water, the Inadvertent ECCS Actuation at Power accident will not degrade into a more serious Condition III event, since these valves will close once ECCS flow has been terminated. It should be noted that the licensees may have qualified these valves in compliance to NUREG-0737, Item II.D.1.
3. If the PSRVs are not designed or qualified for subcooled water relief, the licensees should re-evaluate the Inadvertent ECCS Actuation at Power accident using one or a combination of the following options.

## RECOMMENDED ACTIONS (con't)

Option I: Reduce the maximum ECCS flow used in the safety analysis. Preliminary sensitivity analyses have shown that using less conservative flow may sufficiently delay filling the pressurizer such that the operator action to terminate the accident can be successfully credited.

Option II: Use a less restrictive operator response time. Per ANSI/ANS-58.8-1992, "Time response design criteria for safety-related operator actions," credit can be taken in the analysis for the operator to stop one pump at 7 minutes, a second pump at 8 minutes, and depending on the plant specific design, the third at 9 minutes. Preliminary sensitivity analyses have shown that using these less restrictive operator action times may sufficiently delay or prevent filling the pressurizer.

Option III: Credit the use of one or more PORVs to help mitigate the accident. Preliminary sensitivity analyses have shown that if a water solid pressurizer condition is reached, one PORV should be sufficient to maintain pressure below the PSRV setpoints and prevent discharge of water through the pressurizer safety relief valves. To credit this option, the licensee would have to ensure that at least one PORV is always available (PORV block valve is opened). This option could also be credited if the PORVs are blocked by ensuring that the Emergency Operating Procedures (EOPS) instruct the operators to open at least one PORV block valve before the PORV setpoint is reached. Use of this option may require a change to the plant EOPS and/or the plant technical specifications to ensure that at least one PORV is available since most technical specifications currently allow the PORVs to be isolated during power operation.