IAEA-TECDOC-611

Use of plant specific PSA to evaluate incidents at nuclear power plants

INTERNATIONAL ATOMIC ENERGY AGENCY

USE OF PLANT SPECIFIC PSA
TO EVALUATE INCIDENTS AT NUCLEAR POWER PLANTS
IAEA, VIENNA, 1991
IAEA-TECDOC-611
ISSN 1011-4289

Printed by the IAEA in Austria
June 1991

FOREWORD

One of the possible applications of the plant specific probabilistic safety assessment (PSA) is its use in the analysis of operational events at the plant. The methodological development in that area was initiated recently in the framework of the IAEA's Incident Reporting System where determination of the safety significance of the event is essential for optimizing feedback of operating experience.

This report provides details of the methodology and procedures to be used in event analysis. The report also contains three case studies which have been performed and summarizes lessons learned from those case studies. The results (event probabilities) obtained using plant specific PSA and the results of the analysis of the same events in the framework of the Accident Sequence Precursor (ASP) programmes (generic models) were compared and commented on.

This document is intended to be used by experts involved in both event analysis and PSA. Its general purpose is to summarize current methodological development and encourage and promote use of plant specific PSA in event analysis internationally. Use of plant specific PSA for event analysis would both allow better understanding of the vulnerabilities of the plant given the event occurrence and check the PSA model for appropriateness and completeness. In that respect, the methodology described in this report would benefit both operational experienced analysts and PSA specialists.

This report was prepared during a consultants meeting held in Vienna (24-28 September 1990) by Mr. Patrick W. Baranowsky, United States Nuclear Regulatory Commission (NRC), Washington, D.C., and Mr. Martin B. Sattison, Idaho National Engineering Laboratory, Idaho Falls, Idaho, USA. The IAEA technical officers responsible for this project were Mr. Bojan Tomic and Mr. Valeri Tolstykh from the Safety Assessment Section of the IAEA's Division of Nuclear Safety.

EDITORIAL NOTE

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

A high number of plant specific probabilistic safety assessments (PSAs) which have been completed in the last few years make it appealing to utilize them for other purposes. One of the possible purposes would be the analysis of the operational events occurring at the plant for which the plant specific PSA study exists.

Activities in this area have been initiated by the IAEA in the framework of the Incident Reporting System (IRS). The IRS system has grown considerably in the recent years in terms of quality of the reports and quantity (number of reports shared). Since the events reported to the IRS can differ substantially, optimizing the experience feedback requires selection of those having higher safety significance. In that respect, a tool which would be more precise, such as the recently developed International Nuclear Event Scale, may be needed.

In order to explore the possible application of PSA studies for event analysis, the IAEA organized a consultants meeting in May 1989, which discussed possible approaches and provided a general framework for methodological development. The meeting also proposed that several case studies be performed, including calculation of events probability. The report of the meeting was presented to the TCM of IRS national co-ordinators in October 1989, who supported it and recommended further activities.

The first case study was performed in December 1989. This involved calculation of event probabilities from the PSA report itself, i.e. without use of computerized cut-set manipulation tools, which resulted in somewhat imprecise results. In order to explore the potential of PSA-based event analysis when advanced computerized support is used, the second case study was undertaken and the results are described in this report.

1.2. PURPOSE

The purpose of this work is to develop and document a procedure for the analysis of incidents at nuclear power plants using a plant specific PSA. The intent is to be able to characterize the relative importance of incidents in the light of risks perceived from the original PSA and to derive insights to help evaluate plant specific design and operational problems as incidents occur. This work is not intended to replace the traditional PSA profile of plant core damage likelihood or to provide a revised plant "risk" estimate for comparison of conformance to plant safety objectives. It is intended to provide a method and demonstration of a procedure which can be used to determine safety significance and insights of operating reactor incidents.

1.3. SCOPE AND LIMITATIONS

The selection of reactor incidents and analyses was limited to events which have been found to be risk significant by others and which have occurred at plants for which NRC-sponsored risk assessments [1] have been performed. In addition, it was decided to select events of fairly recent vintage (1988 and 1989) to give more relevance to the results. The existing PSAs were used and were assumed to be up-to-date and accurate. Thus, only PSA model or data changes indicated by the incident were made.

Where potentially extensive modeling or data analyses would normally be required to accurately estimate accident likelihood, a simplified approach was used which allowed timely execution of the event analysis procedure and was also in keeping with the objective of identifying potentially safety significant incidents and associated insights. The methodology employed in the development of the original PSA should be adequate and compatible with the procedures identified herein, if greater precision on certain aspects of the analysis are desired. This is especially true for recovery assessments. Additionally, only a modest effort was made to obtain specific details of plant design and operation brought into question by the incident under reveiw. This aspect could be expanded to satisfy the specific objectives and level of precision of future analyses, but for this exercise, approximations and sensitivity analyses were sufficient to demonstrate the procedure and still properly characterize event significance and insights.

2. INCIDENT ANALYSIS METHODOLOGY AND PROCEDURES

2.1. SELECTION OF INCIDENTS FOR ANALYSIS

The identification of incidents which are potentially significant requires some qualitative screening of incidents to select those of most value for analysis. The methodology and procedures covered in this report are of most value in the analysis of accident sequence precursors. That is, those incidents which involve portions of core damage sequences which are part of a PSA. Generally, any incident, which degrades plant functions that provide portection against core damage or results in unexpected or significant challenges to those functions are candidates for analysis. The methodology, efficiency and speed of tools executing the methodology, and resources available provide the limitations on what can be analysed and how many incidents can be analysed. Past experience with the Accident Sequence Precursors [2] programme in the United States has suggested that incident screening criteria based on PSA insights can be of value to limit the number of plant anomalies and malfunctions for which incident risk analyses would be of value. This would not and should not preclude considering the more complete set of equipment and operations-related problems in trends and patterns analyses or other reliability assessments.

It is suggested that the methodology and procedures used in the case studies in this report are most useful when PSA results and insights tend to raise questions about the incident. These incidents will normally involve safety function failure or degradation, events occurring at a frequency greater than anticipated based on the PSA, multiple failures or degradations in several systems simultaneously, or events that were not well modeled in the PSA.

There are also events which are not amenable to analysis by the methodology and procedures used in this report. These involve incidents outside the scope of the PSA which by their nature are very difficult, if not impossible, to represent within the available PSA framework, model, or methodology. These involve such things as quality assurance programme deficiencies or other programatic breakdowns, loss of design margin, and phenomenological incidents which may raise questions about the functional capability of systems and structures.

2.2. METHODOLOGY AND PROCEDURES

This section documents a methodology for evaluating plant incidents that have a safety significance potential using an existing plant specific PSA. For the three example evaluations in the appendix, the NUREG 1150 PSA models for Sequoyah Unit 1 [3] and Surry Unit 1 [4] were used.

This methodology was demonstrated on the typical large fault tree/small event tree PSA models of NUREG-1150[1]. This type of PSA has the advantage of using sequence cut sets consisting of basic events that can be directly manipulated in the course of the evaluation. However, the approach using a large event tree/small fault tree PSA would be the same, only the specifics of the model manipulations would be different.

This methodology relies heavily on the recalculation of sequence frequencies, regeneration of system and sequence minimal cut sets when needed, and the calculation of several importance measures. These operations generally require the use of a computer. Thus, a computer-based PSA model is almost a must. Hand calculated approximations may be possible if only a copy of the PSA report is available.

The example evaluations presented in this report were performed using microcomputer versions of the NUREG-1150 PSAs. These computer-based models were developed by the US Nuclear Regulatory Commission for uses such as this. The model manipulations and calculations were performed using IRRAS 2.5 [5].

Several other PSA codes exist that can perform similar tasks. Any code would do fine as long as it can regenerate system and sequence cut sets and recalculate sequence results using modified basic event failure data.

The overall approach to incident evaluation using plant specific PSA models involves the following:

- Understanding the incident and its safety implications
- Relating the incident to the PSA models
- Modifying the models to reflect the incident
- Calculating new PSA results and drawing insights from these results.

Understanding the incident and its safety implications requires a knowledge of plant operations and a knowledge about the contents of the specific PSA. Plant operations knowledge allows the analyst to determine if the incident impacted or had the potential to impact a safety function. Knowledge of the specific PSA is required to determine if the potential impacts are within the scope or resolution of the PSA models.

To relate the incident to the PSA, the analyst must determine which accident sequences are involved or could be involved, what fault tree models and basic events model the components or operator actions of concern, and what recovery actions could be applied or are made impossible. Along with this is the need to make changes to the base PSA models to reflect the incident. This could involve restoring accident sequences that were originally truncated out of the final results, changing basic event probabilities, and evaluating new human error rates.

Once the model modifications are made, then they can be processed to determine new results conditional on the existance of the incident.

Finally, analysis of the results must be performed to gain insights pertaining to the safety implications of the incident. These insights include a comparison of the conditional core damage probability to the overall core damage frequency, determination of the new dominant contributors to the core damage frequency, and the new importance of remaining systems/components/ operator actions to prevention of core damage.

The actual analysis steps conducted by this methodology and employed in the three case studies documented in the appendix are:

1. Review the incident. Based on what actually happened during the incident, identify the chronology of events, identify all equipment failures (including those in place at the initiation of the incident), degradations and equipment unavailabilities. Also note all operator actions taken, especially those not covered by procedures and training. It may also be worthwhile to review problems or related conditions which occurred or were identified for some time period (like 1-2 weeks) before and after the incident to be sure that hidden complications are not left unaccounted for in the analysis.

2. Using the event tree models in the PSA, identify all event tree sequences affected by the incident. Use the full event tree models and not just the subset of accident sequences retained by the original PSA. Many times the incident will impact normally very reliable systems that are called upon in very low frequency sequences. To properly identify the affected accident sequences, the analyst must know which event tree top events model the equipment and operator actions involved in the event being analysed. The sequences with a failure branch for at least one of these top events are the sequences of concern.

3. Review the identified PSA sequences and their cut sets to determine if the affected systems and basic events were retained in the original PSA results. Most PSA reports only retain the accident sequences and cut sets that contribute to at least some minimal degree to the core damage frequency. Thus, cut sets consisting of normally very reliable components may not be retained, causing a reduction in the detail of the PSA model in sequences and systems pertaining to the event being analyzed. If the necessary sequences or cut sets were not retained, then they may have to be recreated. This involves generating the cut sets for each system in the missing sequences (if not already in the original model database), being sure to set cut set cutoff criteria so that affected basic events and cut sets are retained. New sequence cut sets must be generated even though the sequence is in the database, if cut sets containing the basic events of concern have been truncated out of the list of dominant cut sets retained in the PSA.

4. With the proper basic events appearing in the cut sets for the appropriate sequences, the next step is to determine the best estimate failure probabilities for all basic events impacted by the incident. Basic events representing failed components should most likely be modeled as a failed house event as opposed to an event with a probability of 1.0. The failed house event will actually modify the Boolean logic of the system or sequence to correctly generate conditional cut sets.* Using this approach, the failed component will not be present in the final cut set equation.

---

* By setting the probability to 1.0, one can introduce overlap between cut sets and double count some failure combinations.

For incidents involving component malfunctions or unavailability but no accident sequence initiating event, the actual or estimated duration at the component unavailability must be taken into consideration. This may be done by multiplying the accident sequence initiator frequency by the amount of time the component was determined to be unavailable. Alternatively the actual or estimated component unavailability could be input to the appropriate cut set basic event. This would require retaining the "failed" component in the cut set equation i.e. not using a failed house event to modify the Boolean logic.

For equipment or operator degradations, detailed systems analysis or human reliability analysis may be required to get an acceptable level of precision and rigor in the revised failure probability. However, conservative screening or bounding values may be used as a first approximation. Only if the results indicate that the screening values are important is more detailed analysis required. One pitfall to watch for is the creation of impossible failure combinations as a result of the incident. The removal of one train of a system from service may make testing and maintenance of the other train impossible or at least administratively restricted. Cut sets containing such test and maintenance actions should be removed from the cut set list, unless evidence associated with the incident or a review of plant operations indicates a reasonable potential for simultaneous outage of redundant trains or components whose outage is restricted by Technical Specifications or other administrative controls.

5. After assigning the proper failure data to the basic events and initiating events, the new accident sequence conditional probabilities can be calculated. This is done by quantifying the new cut set expressions with the new failure data. At this point potentially important sequences which may be affected by incident recovery actions should be identified.

6. Determine the appropriate recovery actions to be applied to the sequence cut sets (if any) based on the events of the incident, personnel available, and plant operating and emergency procedures.

   The determination of the failure probabilities may require detailed analysis. Note that for component unavailability situations which have existed through several shifts, the recovery analysis should consider any significant variations in personnel and skills, or other factors which could impact recovery. The recovery actions credited in the original PSA should be reviewed to assure that the incident being evaluated does not impact the recovery action failure probabilities or render any recovery actions impossible.

7. Calculate new importance measures for the basic events in the new sequence cut set lists. The Fussell-Vesely, risk reduction, and risk increase importance measures can provide the desired insights. The Fussell-Vesely importance indicates the percentage of the conditional core damage probability involving the event for which it has been calculated. The risk reduction ratio indicates the amount of reduction in the conditional core damage probability to be gained if the event was made perfect (failure probability = 0.0). The risk increase ratio indicates the factor by which the conditional core damage probability would go up by if the event was totally unreliable (failure probability = 1.0).

8. Document the analysis, review the results and conduct sensitivity analyses as necessary. The documentation should be clear, concise and traceable. Review the results to determine key contributors in terms of dominant accident scenarios and component/operator actions important to core damage. Use the importance measures to guide the review. Also identify the key features that prevented the incident from becoming more risk significant by using the risk increase importance measure.

   For the key contributors that are subject to judgement or uncertainty, sensitivity analyses may be conducted to determine if the uncertainties could significantly influence the results and may conclusions regarding the incident.

The case studies documented in the appendix followed these steps and serve as examples for the types of analyses and documentation that can come out of this methodology.

3. CASE STUDIES

3.1. INCIDENTS SELECTED FOR CASE STUDIES

Three incidents were selected for the case study applications of the methodology and procedures described in section 2.2. These are:

(1) Potential inoperability of both charging pumps at Sequoyah Unit 2 on February 12, 1988.

(2) Reactor trip with one charging system train and one auxiliary feedwater train unavailable at Sequoyah Unit 2 on May 19, 1988.

(3) Inoperable PORVs at Surry Unit 1 on April 15, 1988.

Incidents (1) and (3) involve system or component reliability and availability degradations which affect vital safety functions - high pressure injection (HPI) at Sequoyah and pressure relief/feed and bleed at Surry. Incident (2) involves a transient with equipment unavailable in two separate system trains which perform complementary safety functions.

The incidents which occurred at Sequoyah Unit 2 were analysed using the Sequoyah Unit 1 PSA. While it is preferred to use the specific PSA model for the plant which experienced the incident, it is believed that the dissimilarities between Units 1 and 2 are not significant for the incidents selected.

3.2. SUMMARY OF RESULTS

A summary of the core damage results for each of the case studies is provided in Table 3-1. This table also provides the original PSA results and the results obtained from the Accident Sequence Precursor (ASP) program analysis of the selected events for comparison. The comparison of the case study with the PSA and ASP results has a different implication and interpretation which are discussed below.

TABLE 3-1

SUMMARY OF CONDITIONAL CORE DAMAGE PROBABILITIES AND COMPARISON WITH PSA AND ASP

	Case Study Results	PSA Results	ASP Results
<u>Case Study 1</u>			
Transients	3.4×10^{-9}	$<10^{-8}$	-
Small LOCAs*	1.4×10^{-6}	$<10^{-8}$	3.8×10^{-4}
ATWS	8.2×10^{-6}	1.5×10^{-6}	-
<u>Case Study 2</u>			
Transients	1.8×10^{-6}	1.5×10^{-6}	1.3×10^{-5}
<u>Case Study 3</u>			
Transients	1.3×10^{-5}	1×10^{-6}	1.5×10^{-5}
Small LOCAs	8.0×10^{-7}	$<10^{-7}$	-
ATWS	2.0×10^{-7}	$<10^{-7}$	-

* Includes steam generator tube rupture sequences

The case study and the ASP results can be compared directly since they are measures of conditional core damage probability given the incident has occurred. However, the ASP results are in the form at an incremental change in the conditional core damage probability where as the case study presents the total sequence core damage probability. The incremental change can be obtained by subtracting the original sequence core damage probability from the new core damage probability. A comparison of the case study and original PSA results involves two somewhat dissimilar quantities. The case study results are in the form of probabilities where as the PSA results are in the form of frequencies or probabilities per year. If the PSA results are integrated over time (e.g. one year), then they can be compared with the conditional core damage probabilities of the case studies. Using one year conveniently allows the core damage frequency to be about the same as the core damage probability. The implications of this comparison are as follows. If the conditional core damage probability of the incident is larger, by about a factor of ten, than the frequency of core damage for the same sequence in the original PSA, there may be plant design and operational factors that are more risky than the original PSA model implies. If the sequence conditional core damage probability results are greater than the total core damage frequency of the PSA, then the perceived plant risk derived from the PSA may be underestimated. These two inferences can only be valid if the PSA and incident analysis are performed with a comparable methodology. The comparative considerations sighted above are based on uncertainties associated with current vintage PSAs. A more rigorous statistical comparison may also be performed, if desired.

In case study 1 it was found that small LOCAs with failure of high pressure injection and ATWS sequences with failure to borate were potentially significant because of the common cause failure of both charging pumps. The PSA did not include a charging pump common cause failure (CCF) event (although other charging system CCF considerations were included). It may be concluded that the affected sequences and importance of the charging pumps were potentially underestimated in the PSA. Corrective actions taken at the plant appear effective in reducing the future CCF of these pumps. The ASP results are much higher because of model differences. Specifically, in the ASP analyses the CCF of the charging pumps was treated as a loss of all high pressure injection, when in fact, the safety injection system was fully operational. Also, ASP models do not include ATWS sequences which were found to be the most affected in the case study.

In case study 2 the conditional core damage probability for the incident was only slightly higher than that derived in the PSA for the same sequences. However, it was observed that this relatively low conditional core damage probability was dependent on operators restoring inoperable systems. Over one order of magnitude in core damage probability reduction were accounted for by the recovery analysis. Because of the uncertainty in this area, inferences regarding the event significance prior to recovery may be of value. The ASP results are much higher because of differences in system models and event recovery. Very limited recovery credit was given in ASP. As part of the case study, information was obtained on the nature of actions required to make either the charging system or AFW train operable. This information was used to estimate a recovery likelihood based on data in Ref. [6].

The third case study involved a potential common cause failure of the PORVs which was included in the PSA. The conditional core damage probability is relatively high, especially for transients where feed and bleed may be required for core cooling. Since the condition of the PORVs would not normally be detected for an operating cycle, which is usually over one year, the risk exposure interval for this event is relatively large. There was very good agreement between the ASP results and the case study as to both conditional core damage probability and sequence characteristics.

4. LESSONS LEARNED FROM THE CASE STUDIES

The analyses performed and described in the previous sections resulted in the identification of several lessons which are as follows:

1. A reasonable and defendable evaluation of safety significance of incidents using PSA is possible if the incident documentation is well prepared and if a well-documented PSA study exists.

2. In cases where the reports do not provide all the information to accurately structure the event (sequence timing, equipment identification, flowsheet diagrams, etc.), PSA experience can be used to develop bounding models that encompass the range of reasonable possibilities.

3. In some cases it was not possible to perform the evaluation using only the existing PSA model results because:

    - the event reported was different from those considered in the PSA (new scenarios created by operator action, unexpected system interactions, different recovery actions).

    - in some cases it was necessary to recreate previously insignificant accident sequences which required additional evaluation and calculation.

In such cases experts were needed with both PSA background to do the necessary additional analysis and with a plant design and operations background to provide additional information concerning the event (level of dependency, common mode, etc.).

4. When the event assessment is aimed at an analysis of the behaviour of the plant as a whole, simultaneous occurrence of additional dependent or independent events have to be considered. The plant-specific PSA is the most appropriate tool for the selection of other credible occurrences since it models the plant design and operation in an integrated way.

5. If the analysis is to be done on a plant for which there is no PSA study available, a simplified model may be used. An example of this approach is the US ASP program. However, the lack of plant-specific details in the models precludes drawing many of the insights associated with risk reduction and component level contributors to risk. Accurate modeling of a specific incident at a specific plant is hindered due to the inability to properly apply revised failure probabilities and recovery actions.

6. Several lessons were related specifically to PSA studies:

   - It was generally concluded that PSA studies vary in the handling of system dependencies (which were not considered in the design phase) and common mode failures. The process of conducting incident evaluations will highlight common mode failures that have occurred but were not properly modeled in the PSA.

   - Event reporting systems such as the IRS and the LER system in the US could be beneficial for PSA practitioners to identify new sequences, new failure modes of components and new recovery actions.

   - Incident evaluations using plant-specific PSAs could be more easily accomplished if the PSA:
     (1) Retained more details of the plant systems and components in the cut sets.
     (2) Retained the logic of the sequences in the event trees, even for sequences truncated out of the PSA.
     (3) Retained the failure data for all basic events in the fault trees, even if they do not show up in any of the sequence cut sets retained after truncation.

Appendix

DETAILS OF CASE STUDIES

CASE STUDY 1

POTENTIAL INOPERABILITY OF BOTH CHARGING PUMPS

Sequoyah Unit 2 (12 February 1988)
LER 328/88-005 R1

Description

While shut down, smoke was discovered coming from the speed increaser unit of centrifugal charging pump (CCP) 2A-A of the charging system. The pump was shut down and pump 2B-B was started.

Upon disassembly of the speed increaser, internal component damage was discovered. Two gland seal retaining bolts inside the lube oil pump had backed out, one bolt coming disengaged and falling to the bottom of the pump casing. The seal allowed air in-leakage and oil outflow resulting in insufficient flow to the speed increaser unit. After pump 2A-A was repaired and returned to service, pump 2B-B was also found to have the same problem. The two trains of the lower head SI system were available.

Additionally, it was discovered that the speed increaser lube oil pumps (1800 rpm) had been mistakenly replaced with lower rated (900 rpm) pumps. These lower rpm pumps had two problems: 1) the type of gears used in the 900 rpm pumps might not be able to adequately pump the oil when being driven at 1800 rpm, causing potential cavitation, and 2) the compression packing seal used in these pumps requires occasional adjustment as the packing wears. If these adjustments are not made, the gland seal bolts will become loose, allowing air in-leakage and resulting in insufficient oilflow to the speed increaser unit.

Corrective action was taken to replace the 900 rpm pumps with the proper 1800 rpm pumps, and the speed increaser internals were inspected and replaced as necessary.

NOTE: In this document the units used are:
psi [6.895 x 10^3 Pa], ^{o} F [-32 x 5/9 ^{o}C] and rpm [1 rev./min].

A summary of initial conditions and equipment failures is provided in Table A1-1. The full incident description (LER 328/88-005 R1) is attached to this case study.

TABLE A1-1

INCIDENT CHRONOLOGY, EQUIPMENT FAILURES, AND OPERATOR ACTIONS

Initial Conditions

Mode 4, 0% power
Reactor Coolant Pressure 350 psi
Reactor Coolant Temperature 247°F

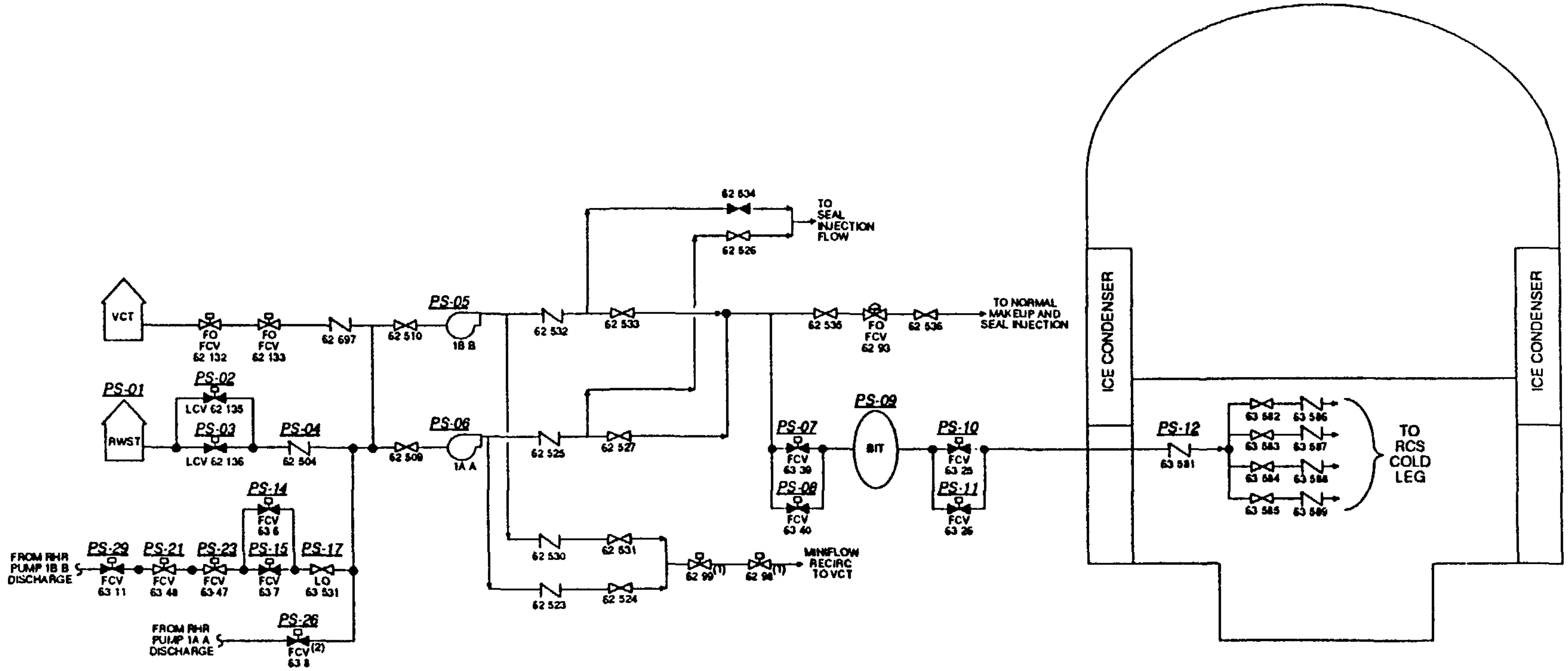
Equipment Failures

2A-A CCP failed on February 12 at 11.33
repaired/operable on February 15 at 18.57

2B-B CCP started on February 12 at about 11.33
tagged out of service on February 17
incipient failure condition noted

Plant Design and Operational Considerations

The charging system consists of two independant trains with high head centrifugal charging pumps. A simplified schematic of the system is shown in Figure A1-1. The charging system, in conjunction with the safety injection system, is used to maintain adequate reactor coolant system inventory for a spectrum of small break loss-of-coolant accidents. If a small break LOCA occurred at full operating pressure and the CCPs were not available, then the operator could depressurize the RCS if necessary, via the pressurizer spray system or by opening the power-operated relief valves, to achieve 1,400 psi RCS pressure where the safety injection (SI) pumps could be utilized for emergency core cooling. The charging system also serves to provide emergency boration for a number of transients including anticipated transients without scram (ATWS) and main steam line break (MSLB).



NOTES: (1) NORMALLY OPEN, POWER REMOVED
(2) WILL NOT OPEN UNLESS TRAINED SUMP ISO. VALVE (FCV 63-73 OR 63-72) IS FULLY OPEN, AND SI MINIFLOW VALVE 63-3 IS FULLY CLOSED OR BOTH SI MINIFLOW VALVES 63-175 AND 63-4 ARE FULLY CLOSED

FIG. A1-1. Simplified schematic of charging system.

Incident Modeling

This incident has been modeled as a failure of both CCPs. The failure probabilities were calculated assuming that a degraded condition which would result in pump failure on demand, would exist for one-half of a surveillance period (360 h) on the average. Since the second pump actually performed its function when demanded while in an incipient failure condition, its failure probability was looked at both assuming that it would have failed on demand if required for a transient or LOCA and with the assumption that the incipient failure condition would not alter appreciably the failure probability derived in the PSA. These two cases provide an upper and lower bound treatment of the potential common mode failure indicated by the incident.

The failure of one or both CCPs potentially affects sequences in the following event trees: T_1, T_2, T_3, T_{sgr}, T_{dc}, ATWS, S_1, S_2 and S_3.

Both high pressure injection (D_1, D_2, D_3, D_4) and high pressure recirculation (H_2) functions are potentially affected by the failure of CCPs. The potentially affected sequences have been identified in Figures A1-2 through A1-10. Because the CCPs were of limited importance in the original PSA, the dominate accident sequence results (cut sets) did not contain terms with basic events involving CCP failure to adequately cover the sequences with functions impacted by CCP failures. Therefore, the original system and function fault trees were reanalysed with high failure probabilities for the CCPs. A revised set of dominant accident sequences and associated cut sets were derived.

The failure of the CCPs was considered to be non-recoverable, and as such, no pump recovery analysis was required. Operator actions involving reactor depressurization and use of the SI system were already included in the model and also required no further analysis. It was recognised that sequences involving top event H_2 were only possible if top event D was successful. In the original PSA, H_2 was mainly composed of operator errors and common cause failures affecting the charging system and safety injection system in the initiation of the recirculation mode. CCP failure to start <u>and</u> failure to run were included in top event D. Since the CCP failure to run considerations were included in the injection phase (D), it is apparent that H_2 sequences will not be noticably impacted as currently modeled in the PSA. Therefore, H_2 sequences were not reanalysed. Also, since the S_2 and S_3 sequences were functionally the same, these two LOCA initiators were combined.

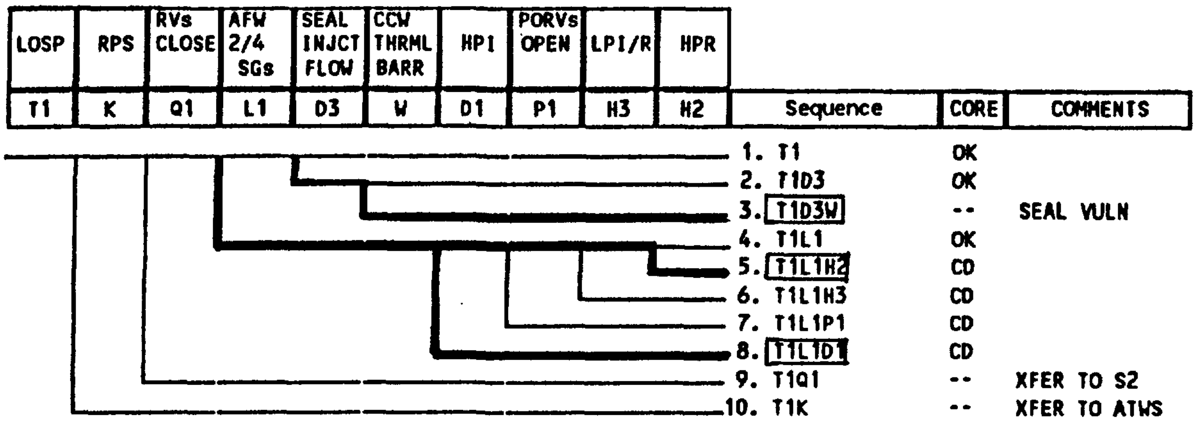


FIG. A1-2. Event tree for T_1 — loss of offsite power.

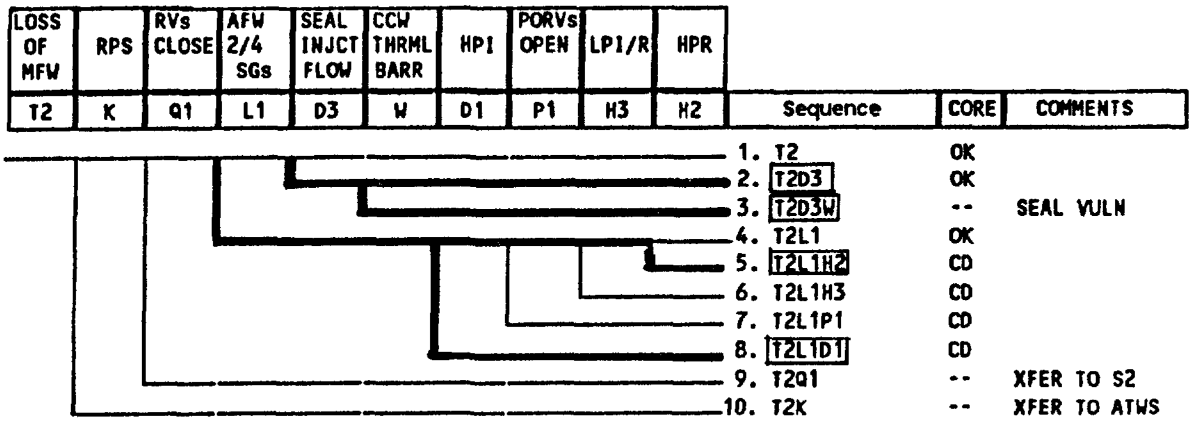


FIG. A1-3. Event tree for T_2 — loss of main feedwater.

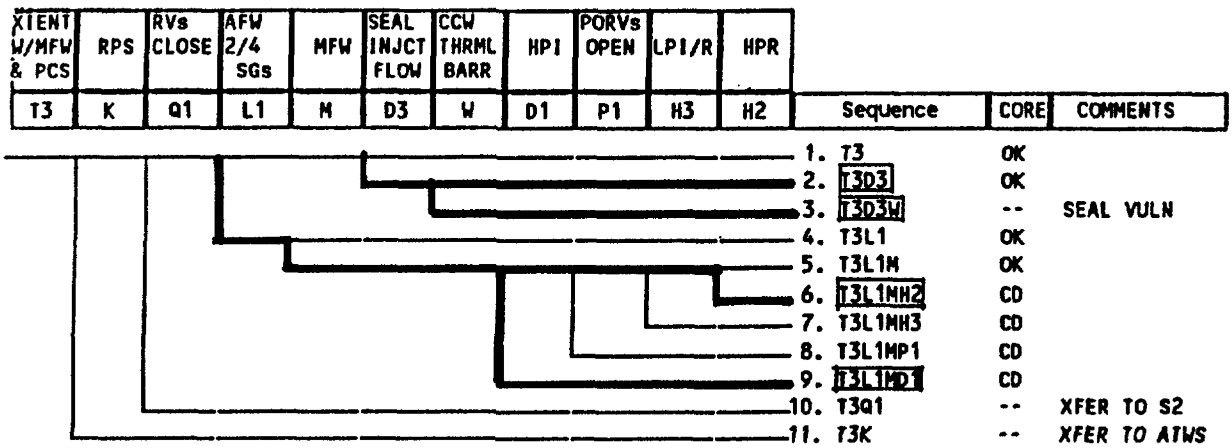


FIG. A1-4. Event tree for T_3 — turbine trip with MFW initially available.

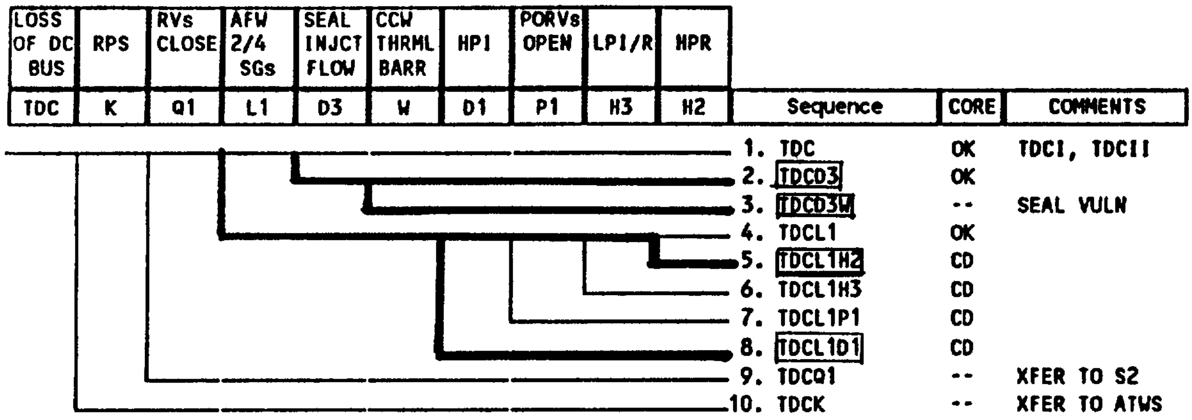


FIG. A1-5. Event tree for T_{DCX} — loss of DC bus.

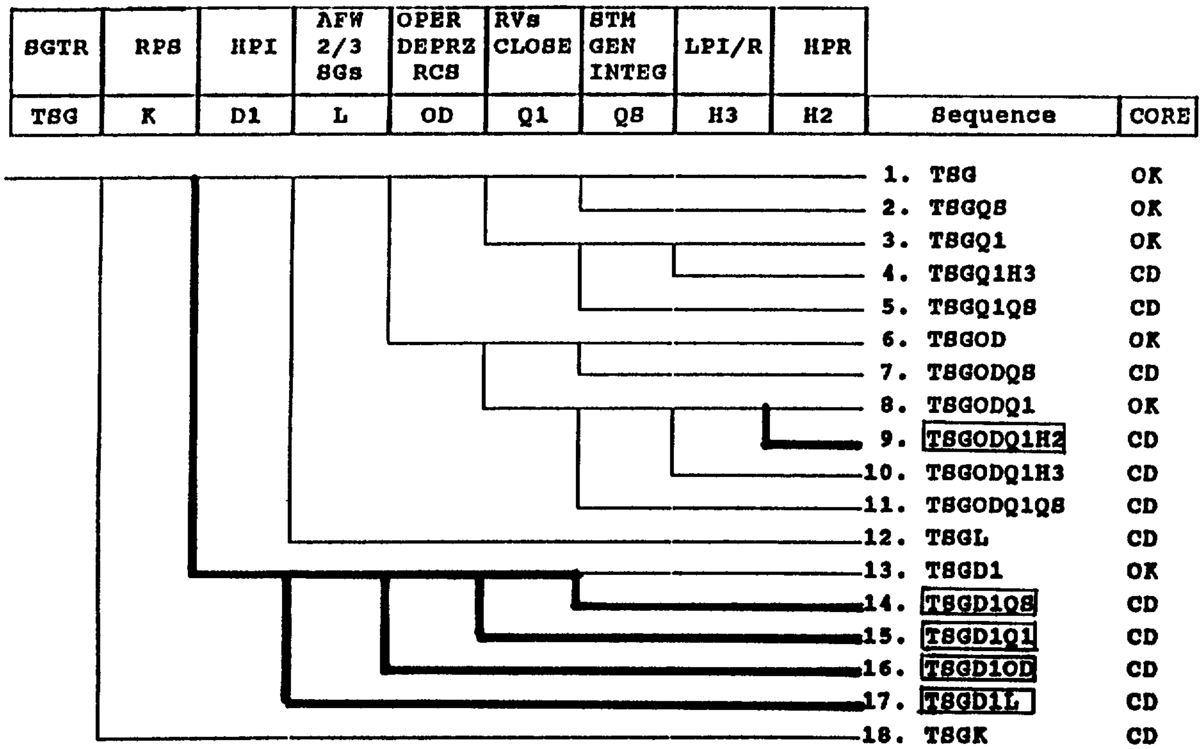


FIG. A1-6. Event tree for T_{SG} — steam generator tube rupture.

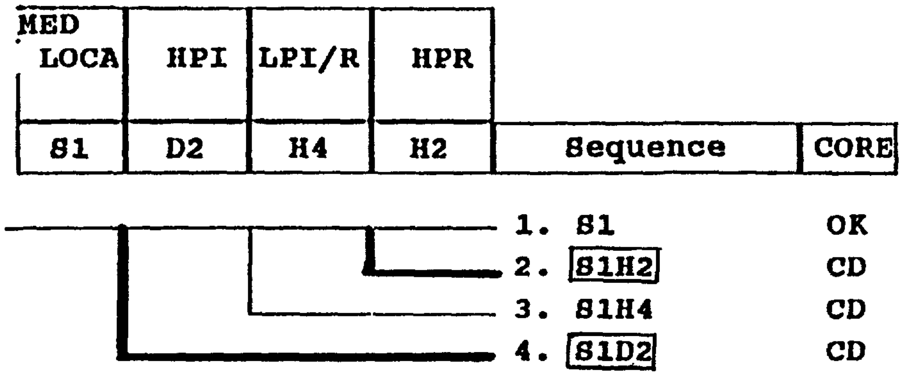


FIG. A1-7. Event tree for S_1 — medium LOCA.

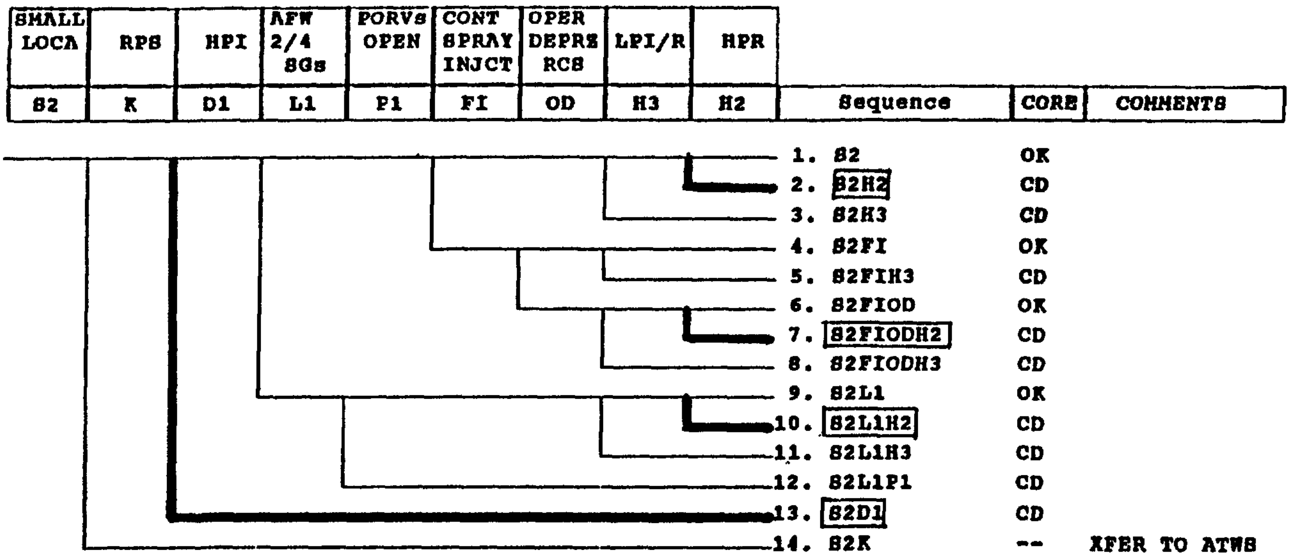


FIG. A1-8. Event tree for S_2 — small LOCA.

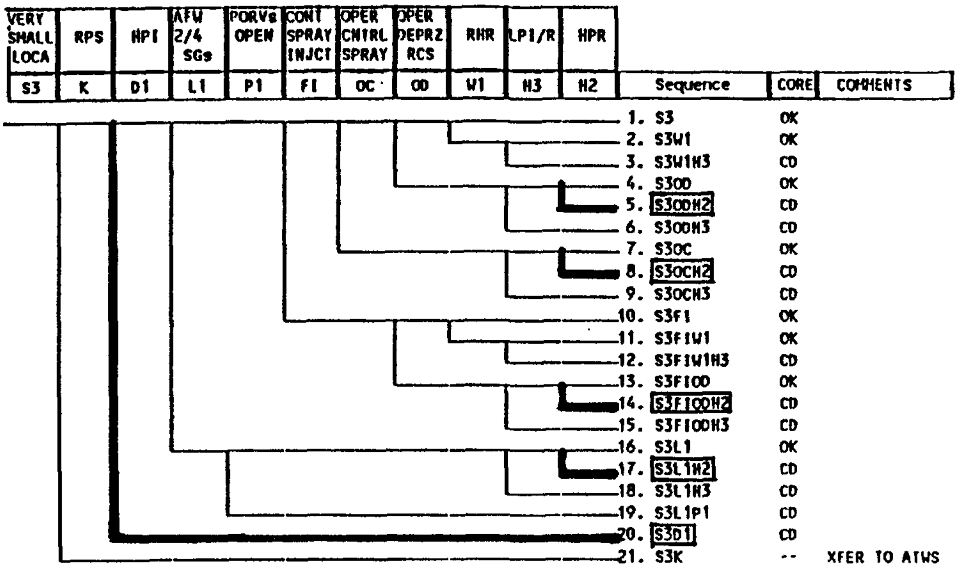


FIG. A1-9. Event tree for S_3 — very small LOCA.

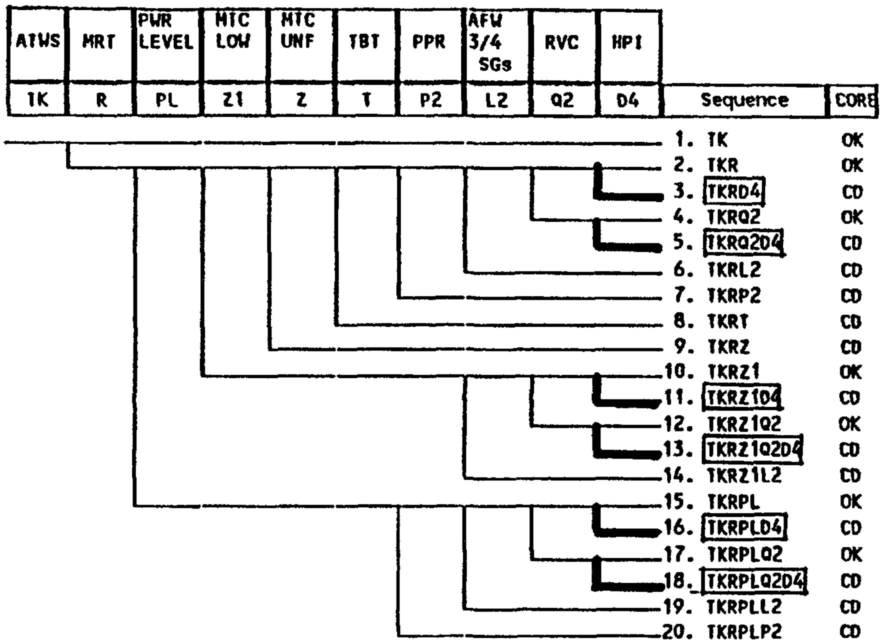


FIG. A1-10. Event tree for T_K — anticipated transient without scram.

No accident sequence initiators occurred during the interval in which the CCPs were potentially inoperable.(i.e. incapable of performing their design basis function given the occurence of an accident initiator). Therefore it was necessary to estimate the likelihood of an accident sequence initiator occuring during that interval. It was assumed that the CCPs were shown to be fully operational during the previous surveillance test about one month earlier. It was further assumed that the CCP degradation occured as a constant failure rate process. Under these conditions the CCPs would be in a failed state for one-half the surveillance interval at one month or 4.1×10^{-2} years. The frequency of each accident sequence initiator ($years^{-1}$) was multiplied by the calculated exposure interval to derive an estimate of their probability of occurance during the time the CCPs were assumed to be inoperable.

The basic event and initiating event probabilities used in the analysis are provided in Table A1-2.

TABLE A1-2. BASIC EVENT PROBABILITIES

Event	PSA	Incident
CHP-MDP-FR-2AA charging pump 2A-A fails to run	3×10^{-5}	house event (1.0)
CHP-MDP-FS-2BB charging pump 2B-B fails to start	3×10^{-3}	house event (1.0) 4.1×10^{-2} (sensitivity 1) 3×10^{-3} (sensitivity 2)
IE Initiating Events		$IE \times 4.1 \times 10^{-2}$

Analysis Results

The conditional probability associated with this incident is about 1×10^{-5}. The dominant sequences involve ATWS and small LOCAs including steam generator tube ruptures. A listing of the dominant sequences and associated probabilities is provided in Table A1-3. Supplemental sensitivity analyses were performed to investigate the sensitivity of the assumption that the 2B-B CCP would have failed if demanded during an accident. This pump

TABLE A1-3. ACCIDENT SEQUENCE CONDITIONAL PROBABILITIES

Sequence	Conditional Probability	Sequence	Conditional Probability
$T_1\ L_1\ D_1$	3.3×10^{-9}	$S_1\ D_2$	2.1×10^{-7}
$T_3\ L_1\ M\ D_1$	1.0×10^{-10}	$S_2\ D_1$	5.9×10^{-7}
$T_{dc}\ L_1\ D_1$	2.0×10^{-11}	Total	9.6×10^{-6}
$T_{sg}\ D_1\ Q_s$	6.3×10^{-7}	Sensitivity 1	5.9×10^{-7}
$T_{sg}\ D_1\ Q_1$	1.9×10^{-9}	Sensitivity 2	2.4×10^{-7}
$T_{sg}\ D_1\ OD$	1.3×10^{-8}		
$T_{sg}\ D_1\ L$	7.8×10^{-10}		
$T_k\ R\ D_4$	4.5×10^{-6}		
$T_k\ R\ Q_2\ D_4$	6.2×10^{-7}		
$T_k\ R\ Z_1\ D_4$	2.2×10^{-6}		
$T_k\ R\ Z_1\ Q_4\ D_4$	3.1×10^{-7}		
$T_k\ R\ PL\ D_4$	4.5×10^{-7}		
$T_k\ R\ PL\ Q_2\ D_4$	6.2×10^{-8}		

Note: S_2 includes S_3 initiator frequency actually did operate after pump 2A-A failed, but was not subjected to accident demands. In the first sensitivity case, the coincident failure of CCP 2B-B was assumed to be loosely coupled to that of CPP 2A-A with an independent probability of failure represented by the unavailability equal to one-half the surveillance interval. This value is 4.1×10^{-2}. When this value is used, the conditional core damage probability becomes 5.9×10^{-7}. For the second sensitivity case, the failure probability of pump CCP 2B-B was assumed to be essentially unaffected by the degraded condition that was found during subsequent inspection of the pump. The base PSA failure probability of 3×10^{-3} was used. The resultant core damage probability is 2.4×10^{-7}.

The importance of the CCP failures(s) associated with this event is approximately bounded by the common mode failure case of 10^{-5} and the independent failure case of 2.4×10^{-7}. The available evidence implies that the common mode failure assumption most closely represents the risk implications of the incident as reported.

Since the charging pumps have a significant impact on emergency boration, it is not surprising that ATWS sequences become most important with the failure of both CCPs. This is followed by the much less significant small LOCA and steam generator tube rupture with safety injection system failure. The reactor protection system, which was already of relatively high importance, rises even higher. This is also true for a number of potential common cause failure points in the safety injection system (i.e. MOV-63-22, CKV - 6351, and both SI pumps).

It is interesting to note that the original PSA did not include a common cause failure of the charging pumps in the logic model. Only failure to run for the operating CCP and an independent failure to start, run or test and maintenance unavailability was included for the standby pump.

NRC Form 366
(9-83)

U.S. NUCLEAR REGULATORY COMMISSION
APPROVED OMB NO. 3150-0104
EXPIRES 8/31/88

LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)	DOCKET NUMBER (2)	PAGE (3)
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	1 OF 0 8

TITLE (4) Loosening Of Gland Seal Bolts On Speed Increaser Lube Oil Pumps Causes A Potential Inoperability Of Both Unit 2 Centrifugal Charging Pumps

EVENT DATE (5)			LER NUMBER (6)			REPORT DATE (7)			OTHER FACILITIES INVOLVED (8)	
MONTH	DAY	YEAR	YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	MONTH	DAY	YEAR	FACILITY NAMES	DOCKET NUMBER(S)
0 2	1 2	8 8	8 8	0 0 5	0 1	0 4	0 8	8 8	Sequoyah, Unit 1	0 5 0 0 0 3 2 7
										0 5 0 0 0

OPERATING MODE (9): 4

POWER LEVEL (10): 0 0 0

THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10 CFR §: (Check one or more of the following) (11)

20.402(b)	20.405(c)	50.73(a)(2)(iv)	73.71(b)
20.405(a)(1)(i)	50.36(c)(1)	XX 50.73(a)(2)(v)	73.71(c)
20.405(a)(1)(ii)	50.36(c)(2)	50.73(a)(2)(vii)	OTHER (Specify in Abstract below and in Text, NRC Form 366A)
20.405(a)(1)(iii)	50.73(a)(2)(i)	50.73(a)(2)(viii)(A)	
20.405(a)(1)(iv)	50.73(a)(2)(ii)	50.73(a)(2)(viii)(B)	
20.405(a)(1)(v)	50.73(a)(2)(iii)	50.73(a)(2)(x)	

LICENSEE CONTACT FOR THIS LER (12)

NAME	TELEPHONE NUMBER
Tom Rogers B. E. Kilgore, Plant Operations Review Staff	AREA CODE 6 1 5 — 8 7 0 - 7 0 8 7

COMPLETE ONE LINE FOR EACH COMPONENT FAILURE DESCRIBED IN THIS REPORT (13)

CAUSE	SYSTEM	COMPONENT	MANUFACTURER	REPORTABLE TO NPRDS	CAUSE	SYSTEM	COMPONENT	MANUFACTURER	REPORTABLE TO NPRDS

SUPPLEMENTAL REPORT EXPECTED (14)

YES (If yes, complete EXPECTED SUBMISSION DATE) — XX NO

EXPECTED SUBMISSION DATE (15): MONTH | DAY | YEAR

ABSTRACT (Limit to 1400 spaces, i.e., approximately fifteen single-space typewritten lines) (16)

On February 12, 1988, at approximately 1133 EST, smoke was discovered coming from the speed increaser unit for the 2A-A centrifugal charging pump (CCP). Immediately, the 2B-B CCP was started, and the 2A-A CCP was stopped. Upon disassembly of the 2A-A CCP speed increaser, much of the internals were found damaged. Further investigation found the two gland seal (GS) retaining bolts inside the speed increaser lube oil pump (SILOP) backed out allowing the GS to loosen. The GS being loosened caused reduced oil flow to the speed increaser internals and ultimate damage. The 2B-B and 1B-B SILOPs were inspected, and the same GS bolts as on the 2A-A pump were found loosened. The cause of the bolts backing out was determined to be lack of a periodic adjustment of the GS bolts. It was discovered during investigation that the original SILOPs for 2A-A, 2B-B, and 1B-B CCPs had been replaced with incorrect SILOPs. The original 1A-A SILOP was not replaced with an incorrect SILOP. The replacement SILOPs had been ordered using an incorrect part number in April 1985. The replacement SILOPs for 1B-B, 2A-A, and 2B-B were rated for 900 rpm and incorporated a compression packing seal which requires periodic adjustment as the packing wears. The original SILOPs were rated for 1,800 rpm and incorporated a mechanical seal which does not require adjustment. The major cause of this event was that the replacement SILOPs for 1B-B, 2A-A, and 2B-B were the wrong SILOPs that incorporated the packing seal, and no program was in place to periodically tighten the gland bolts. The 2A-A SILOP was replaced with an 1,800 rpm pump on February 15, 1988, and two new pumps (1,800 rpm) were procured for 1B-B and 2B-B and installation was completed on March 7, 1988. The 1A-A SILOP mechanical GS bolts were insepcted on April 7, 1988, and found to be satisfactory. To prevent recurrence, TVA has a new procurement program in place which provides additional independent review/verification of all plant initiated procurement documents.

NRC Form 366A (9-83)

U.S. NUCLEAR REGULATORY COMMISSION

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

APPROVED OMB NO 3150-0104
EXPIRES 8/31/88

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6)			PAGE (3)
		YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	8 8	— 0 0 5	— 0 1	0 2 OF 0 8

TEXT (If more space is required, use additional NRC Form 366A's) (17)

This revision is being submitted to provide an update of completed corrective actions and a restatement of the event analysis.

DESCRIPTION OF EVENT

On February 12, 1988, at approximately 1133 EST with unit 2 in mode 4 (0 percent power, 350 psig, 247 degrees F) and unit 1 in mode 5 (0 percent power, 4 psig, 123 degrees F), smoke was discovered coming from the speed increaser unit on the 2A-A (unit 2, train "A") CCP (EIIS Code BQ). Immediately, the 2B-B (unit 2, train "B") CCP was started, and the 2A-A CCP was shut down. The CCPs are utilized in the boron injection system for reactivity control and in the emergency core cooling system (ECCS) (EIIS Code BQ). Both pumps are required to be operable in modes 1 through 4 by the plant technical specifications (TSs). Since unit 2 was in mode 4 at the time, the action statement for TSs 3.1.2.2 and 3.1.2.4 were complied with immediately. This involved restoring both charging pumps to operable status within seven days or bring the unit to cold shutdown within the next 30 hours.

Disassembly of the 2A-A CCP speed increaser box was started later the same night, and upon disassembly, much of the internals were found damaged. Upon further investigation of the cause, it was discovered that the two gland seal retaining bolts inside the speed increaser lube oil pump had backed out with one bolt completely disengaged from the bolt hole and lying in the bottom of the pump casing. The lube oil pump is mounted on the side of the speed increaser and is driven by the speed increaser low speed shaft. The pump recirculates oil in the speed increaser to lubricate the internal moving parts and to serve as a cooling medium in removing heat. The lube oil pump is a rotary gear type and incorporates a gland seal to seal around the shaft. The seal is provided to isolate the pump internal pressure from the external atmosphere.

The bolts being backed out allowed the gland seal to loosen and not provide the seal in which it was designed to perform. After evaluation of the pump design and discussions with the supplier (Westinghouse), it is theorized that the loosening of the gland seal allowed air to be drawn in, via the speed increaser housing, mixing with the oil and/or allowed oil from the pump to be forced through the loosened gland seal bypassing the normal flow path to the speed increaser internals. These conditions caused reduced oil flow to the speed increaser internals and ultimate damage to the internals. The speed increaser internals were replaced as necessary, and the lube oil pump was replaced with one from a spare speed increaser unit. After reassembly, postmaintenance tests were performed on the 2A-A CCP and speed increaser unit, and the pump was returned to operable status at 1857 EST on February 15, 1988.

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6) YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	PAGE (3)
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	8 8	— 0 0 5 —	0 1	0 3 OF 0 8

TEXT (If more space is required, use additional NRC Form 366A's) (17)

As additional preventive actions, the 2B-B (unit 2, train B) CCP was tagged out of service on February 17, 1988, to inspect the lube oil pump gland seal for a similar condition. Upon disassembly, the gland seal bolts were also found backed out similarly to the train A pump. The bolts were retightened and a locktite sealant installed to prevent the bolts from loosening again during operation. Concurrence was obtained from Westinghouse that this would be an acceptable method for securing the bolts.

The 2B-B CCP was declared operable at 0500 EST on February 18, 1988. After evaluation of the similar condition on both unit 2 CCPs, it was determined that this condition alone could have prevented the fulfillment of this system's safety function. At 1218 EST on February 19, 1988, NRC was notified by phone of this condition in accordance with 10 CFR 50.72, paragraph b.2.iii. As further preventive measures, work requests (WRs) were prepared to inspect the speed increasers lube oil pumps on both unit 1 CCPs (WR B257714 for 1A-A and WR B257712 for 1B-B). On February 24, 1988, the oil pump for 1B-B was removed, and the gland seal bolts were found only fingertight. The bolts were retightened and locktite sealer applied. The 1B-B speed increaser was also disassembled, and no damage was noted.

CAUSE OF EVENT

The cause of the 2A-A CCP speed increaser internals damage is attributed to the lube oil pump gland seal bolts backing out and subsequent loosening of the gland seal. This condition ultimately caused reduced oil flow to the speed increaser internals.

An immediate investigation was also initiated to determine the cause of the gland seal bolts backing out. Westinghouse was consulted about this event, and no other conditions of this nature had been reported by other customers.

Past vibration level charts on the speed increaser unit were reviewed, and no abnormal vibration levels were noted that should have caused the bolts to loosen. A 35 mil axial vibration was noted on the 2B-B speed changer in mid January 1988, but this condition was not considered to be the root cause of the bolts backing out since this vibration was only found on one pump/speed changer unit. The main cause of this vibration was found to be a misalignment of the electric motor to speed increaser low speed shaft coupling and was corrected on January 14, 1988.

NRC Form 366A (9-83)

U.S. NUCLEAR REGULATORY COMMISSION

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

APPROVED OMB NO. 3150-0104 EXPIRES 8/31/88

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6) YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	PAGE (3)
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	8 8	— 0 0 5	— 0 1	0 4 OF 0 8

TEXT (If more space is required, use additional NRC Form 366A's) (17)

Maintenance records were reviewed, and no records were found to indicate that any maintenance had been performed on the internals of the pumps that could have contributed to the bolts loosening. However, maintenance records did indicate that all (1A-A, 1B-B, 2A-A, 2B-B) the lube oil pumps had been replaced with complete new pumps on different occasions. At the time of each replacement, it was thought that the replacement pumps were identical to the original lube oil pumps. However, after further investigation and conversations with the manufacturer, it was discovered that some of the replacement pumps used on past occasions were not the correct type pump for this application. It was discovered that two different pumps are made in this style. One pump is rated for 900 rpm maximum speed and typically incorporates a compression packing-type seal which requires occasional adjustment of the gland bolts as the packing wears. The other pump is rated for 1,800 rpm maximum speed and typically incorporates a mechanical-type seal which does not require any periodic adjustment. The oil pumps in this application are driven at approximately 1,800 rpm by the speed increaser low speed shaft. The original lube oil pumps were the 1,800 rpm rating and incorporated the mechanical seal. An inspection was performed on all the speed increasers (1A-A, 1B-B, 2A-A, 2B-B) to determine which pumps were in place at the time of this event. The speed increaser for 1A-A CCP was the only one incorporating the correct lube oil pump (1,800 rpm). The other three (1B-B, 2A-A, 2B-B) had the incorrect lube oil pump (900 rpm). According to the manufacturer, the only structural difference between the two pumps is the type of internal gears used and the type of seal. The 900 rpm rated pump uses spur-type gears internally which have teeth radially arrayed on the rim parallel to the axis and typically incorporate a compression packing seal. The 1,800 rpm rated pumps incorporate helical-type (spiral) gears and typically incorporate a mechanical seal. Using the 900 rpm rated pumps in this application presents two problems (1) the type of gears used in the 900 rpm pump may not be able to adequately pump the oil when being driven at 1,800 rpm and some cavitation may occur and (2) the compression packing seal used in these pumps requires occasional adjustment as the packing wears. The major cause in this event was the fact that the wrong pumps were being used on the speed increasers for 1B-B, 2A-A, and 2B-B CCPs that incorporated the compression packing seal. Maintenance section did not have a program in place to periodically adjust the gland bolts as the packing wears because it was not known that a compression packing was used. This allowed the packing wear to go undetected, and driving the pumps at a higher speed than the rating caused the packings to wear quicker than normal. Ultimately, this condition allowed the gland and gland bolts to loosen. The incorrect pumps being used was caused by maintenance personnel using an incorrect part number when ordering replacement pumps in April 1985. Even though the 1,800 rpm requirement was noted on the purchase contract, the part number for the 900 rpm pump was listed, and the 900 rpm pump was received. Since the lube oil pumps were originally supplied as an integral part of the speed changer units, minimal literature was available specifically for the lube oil pumps. In 1985, the process of ordering parts consisted of a quality assurance review of the maintenance engineer's purchase request. A technical evaluation with an independent review was not included in the program.

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6) YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	PAGE (3)
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	8 8	— 0 0 5	— 0 1	0 5 OF 0 8

TEXT (If more space is required, use additional NRC Form 366A's) (17)

ANALYSIS OF EVENT

This event is being reported under 10 CFR 50.73, paragraph a.2.v, as a condition that alone could have prevented the fulfillment of a safety function that is needed to shut down the reactor and maintain it in a safe shutdown condition or to mitigate the consequences of an accident.

The similar condition of the gland seal bolts being backed out on both unit 2 CCPs and on one unit 1 CCP is a condition that alone could have prevented the fulfillment of the CCPs safety function. The CCPs are required as part of the boron injection system to ensure negative reactivity control is available.

During modes 1 through 4, both CCPs are required to ensure adequate shutdown margin during a cooldown to 200 degrees F, when an assumed single failure is considered. The CCPs provide shutdown margin by injecting the boron injection tank contents into the RCS. The consequences of a cooldown from a main steam line break (MSLB) has been analyzed in the Sequoyah Final Safety Analysis Report (FSAR). The analysis assumed end of core life at no load with equilibrium xenon conditions at the time of a MSLB. Upon recognizing the MSLB by the reactor protection system and the emergency safety feature actuation system, a reactor trip is assumed to occur with the most positive reactive rod cluster assembly stuck in the fully withdrawn position. The single failure assumed is one that would cause a CCP failure, and thus, the boron injection tank contents are assumed to be injected into the RCS by the redundant train. This analysis has shown that a return to criticality occurs following the reactor trip until the boron from the boron injection tank enters the core region. This analysis showed however that peak core levels would be well below the nominal full power level, the lowest departure from nucleate boiling ratio would be greater than 1.30, and the maximum linear heat rate would be less than 10 kw/ft. However, if both CCPs failed during a postulated MSLB, the boron injection tank contents would not be injected and therefore, would place the core in a condition outside of the FSAR analysis. During an actual event, there are additional sources of boron available that are not given credit in the FSAR analysis. These other sources of boron include the ECCS water supply in the refueling water storage tank, the upper head injection system, and the cold leg accumulators. A power increase would also be limited due to the effects of the moderate temperature coefficient and the doppler coefficient as heat is generated from the fission process. The plant conditions existing at the time the smoking speed increase was discovered was not conducive to a return to criticality condition from a cooldown event, however, because of the existing boron concentration in the RCS. The boron concentration has been maintained in both units at approximately 2,000 ppm during the current shutdown period. A boron concentration of 2,000 ppm provides the adequate shutdown margin to preclude the reactor from attaining criticality from a cooldown occurrence. Operating boron concentrations would be less than 1,200 ppm dependent upon the time of core life.

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6)			PAGE (3)
		YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	8 8	— 0 0 5 —	0 1	0 6 OF 0 8

TEXT (If more space is required, use additional NRC Form 366A's) (17)

In modes 1 through 3, both CCPs are required, and in mode 4 one CCP is required for ECCS. Emergency core cooling capability is required in modes 1 through 4 in the event of a loss of coolant accident (LOCA). The CCPs are utilized in the high head injection phase of ECCS for RCS pressures above approximately 1,400 psig at which time the safety injection (SI) pumps can be utilized. If a small break LOCA occurred at full operating pressure and the CCPs were not available, then the operator could depressurize the RCS if necessary, via the pressurizer spray system or by opening the pressurizer power operated relief valves, to achieve 1,400 psig RCS pressure where the SI pumps could be utilized for emergency core cooling.

Therefore, assuming worst-case condition of both CCPs being inoperable, even at full operating conditions, alternate means would have been available to provide a means of obtaining a safe shutdown and to mitigate the consequences of an accident. Even though the potential existed for both CCPs to become inoperable, one pump was maintained in operation at all times on both units since the discovery of the condition on the 2A-A CCP.

CORRECTIVE ACTIONS

Immediate corrective actions were to replace the 2A-A CCP speed increaser lube oil pump and retighten the gland bolts on the lube oil pumps for 2B-B and 1B-B. Locktite sealant was applied to the gland bolts on all three pumps. Also, the speed increaser internals were inspected and replaced as necessary for the three same CCPs. Condition Adverse to Quality Reports (CAQRs) (SQP 880161 and SQP 880188) were also initiated to document the problems identified in this report and track the resolutions.

Immediately upon discovery of the incorrect pumps being procured in April 1985, an inspection was performed to determine which type of pumps were in place at the time of this event and which type was installed on 2A-A during the recent (February 15, 1988) replacement. It was discovered that at the time of this event, only the speed increaser lube oil pump for 1A-A CCP was the correct type (1,800 rpm). The other three (1B-B, 2A-A, 2B-B) were the incorrect type (900 rpm) for this application and incorporated the compression packing seal. However, the new pump installed February 15, 1988, on the 2A-A unit was the correct type pump (1,800 rpm) because it had been removed from a spare speed increaser unit. Therefore, at present, only the 1B-B and 2B-B speed increasers still have the incorrect lube oil pumps installed. Since the 1B-B speed increaser was still disassembled for inspection and unit 1 only requires one CCP in mode 5, immediate operability of the 1B-B pump was not a concern. An immediate operability evaluation of 2B-B CCP was performed which included consulting Westinghouse (the speed increaser supplier). After evaluation, it was determined that the 2B-B CCP is capable of performing its intended safety-related function until new 1,800 rpm rated pumps could be procured (expected maximum duration of two weeks). This determination was made with concurrence from Westinghouse based on past adequate operating time of the 900 rpm pumps and with the requirement of special monitoring to be initiated on the speed increaser parameters (vibration, bearing temperature, and oil analysis) when the pump is running.

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6)			PAGE (3)
		YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	8 8	— 0 0 5 —	0 1	0 7 OF 0 8

TEXT (If more space is required, use additional NRC Form 366A's) (17)

This special monitoring was initiated immediately on the 2B-B CCP speed increaser to provide indication of degraded performance. If indications of degraded performance are noted based on margins provided by Division of Engineering (DNE), the CCP will be declared inoperable and the appropriate Limiting Condition for Operation (LCO) action complied with. This evaluation was documented on a Safety Evaluation form (B25 880302 579) performed by DNE and a Justification for Continued Operation (JCO) form as part of CAQR SQP 880188.

Two new 1,800 rpm rated lube oil pumps were ordered on an emergency basis and the installation of them on the 1B-B and 2B-B speed increasers was completed on March 7, 1988. These pumps were installed under WRs B257712 and B247090.

Westinghouse has been consulted on the 1,800 rpm lube oil pumps to determine if preventive maintenance is required on the mechanical seal gland package to ensure loosening of the gland seal does not occur. Westinghouse does not recommend any preventive maintenance on these type seals and a review of their operating history by Westinghouse did not indicate that preventive maintenance is required. Therefore, an inspection of the mechanical seal gland bolts will not be incorporated into the preventive maintenance program.

To prevent recurrence, TVA has a new procurement program in place which provides additional independent review/verification of all procurement documents initiated in the plant. The procurement process is provided in SQA-45, "Procurement of Materials, Components, Spare Parts, and Service," and TI-110, "Procurement of Replacement Items for Use In Permanent Equipment, Systems and Structures," approved on October 19, 1987. The Contract Engineering Group (CEG) performs this function by reviewing all plant initiated reorder procurement documents against the current design specifications. The CEG technical review includes a verification of part numbers provided by the requesting organization against the latest controlled drawing and/or the vendor manual. This verification is then independently reviewed by an engineer and approved by a CEG manager before the procurement package is submitted to the Quality Assurance organization for their review. The latest revision (revision 29) of SQA-45, "Procurement of Materials, Components, Spare Parts, and Services," also requires additional identifying specifications on all purchase request documents which are reviewed in the same manner as the part numbers. Also, Maintenance Instruction (MI)-12.3.1, "Centrifugal Charging Pump Speed Increaser Inspection and Maintenance," was revised on March 30, 1988, to add instructions for verifying the correct lube oil pump when making replacements.

NRC Form 366A (9-83)

U.S. NUCLEAR REGULATORY COMMISSION
APPROVED OMB NO. 3150-0104
EXPIRES 8/31/88

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6) YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	PAGE (3)
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	8 8	— 0 0 5 —	0 1	0 8 OF 0 8

TEXT (If more space is required, use additional NRC Form 366A's) (17)

ADDITIONAL INFORMATION

Centrifugal Charging Pump Speed Increaser - Westinghouse High Speed Gear Drive Model Su-1023-8X.

Speed Increaser Lube Oil Pump (1,800 rpm rating) - Westinghouse Style 159A422G28, Manufactured by Browne & Sharpe Co., Part Number 713920-3 (No. 2S).

Speed Increaser Lube Oil Pump (900 rpm rating) - Browne & Sharpe Co., Part Number 713902-1 (No. 2).

There have been no previous reportable occurrences involving the CCPs speed increaser units.

0879Q

CASE STUDY 2

REACTOR TRIP WITH ONE HIGH PRESSURE INJECTION TRAIN AND ONE AUXILIARY FEEDWATER TRAIN UNAVAILABLE

Sequoyah Unit 2 (19 May 1988)
LER 328/88-23 R1

Description

While at 72% power, operators were troubleshooting a high level indication of the No. 3 heater drain tank level indicator. The heater drain tank sight glass had become clogged and was providing erroneous level indication. As operators attempted to reduce the level in the tank, the heater drain tank suction pumps began to cavitate and subsequently tripped. This immediately initiated an automatic turbine load reduction, which led to balance of plant fluctuations that eventually caused a reactor trip. In addition to a reactor trip, plant cooldown was exacerbated by steam leaking through the "A" main feedwater pump throttle valve and an intermittent opening of a steam dump valve to the condenser. During the reactor trip and following recovery, the 2A-A centrifugal charging pump (CCP), and the 2B-B auxiliary feedwater pump were unavailable due to surveillance testing and maintenance.

A summary of the incident chronology, equipment failures, and operator actions is provided in Table A2-1. A more complete description (LER 328/88-23 R1) is attached to this case study.

Plant Design and Operational Considerations

A reactor trip at higher power levels will generally satisfy the logic to isolate main feedwater as was the case in the May 18 incident. Main feedwater would be recoverable by operators from the control room, if other malfunctions do not affect its operability.

The auxiliary feedwater system (AFW) consists of two motor-driven pump trains and one steam turbine-driven pump train. A simplified schematic of the system is shown in Figure A2-1. All AFW pumps will start automatically following a reactor trip, however, only one of three AFW pumps feeding any two steam generators is required.

TABLE A2-1

INCIDENT CHRONOLOGY, EQUIPMENT FAILURES AND OPERATOR ACTIONS

Initial Conditions

Reactor at 71.7% power, 2234 psi, 566^{o}F

No. 3 Heater Drain Tank pumps tripped due to cavitation

A main feedwater pump in automatic control

B main feedwater pump in manual control

Steam generator 3 low level bistable tripped (out of service)

2A-A centrifugal charging pump inoperable for SI-40.1

2B-B AFW pump inoperable for SI-298.2

Chronology

Operators attempting to control S/G level due to No. 3 HDT pumps tripping at 14:08

Bypass regulator valve opened 20%, then MFW to loops 2,3, and 4 closed

Steam flow/feed flow mismatch resulted in reactor trip at 14:13 (S/G 3 low level)

Main feedwater isolated on reactor trip coincident with low T (average)

Available AFW pumps (MDP, TDP) started

Letdown isolated at 17% pressurizer level

Hotwell level declining

Operator Actions

Manual control of main feedwater train B, unsuccessful

Recovery from trip initiated using ES-0.1, "Reactor Trip Response, Units 1 & 2".

Equipment Failures and Anomalies

2A-A CCP unavailable, potentially recoverable

2B-B AFW pump unavailable, potentially recoverable

Steam dump valve 2-FCV-1-104 intermittently opened without demand

No. 1 feedwater regulator valve failed in the as-is position

A main feedwater pump steam valve leaked

Vacuum drag valve 2-LCU-2-9 malfunctioned

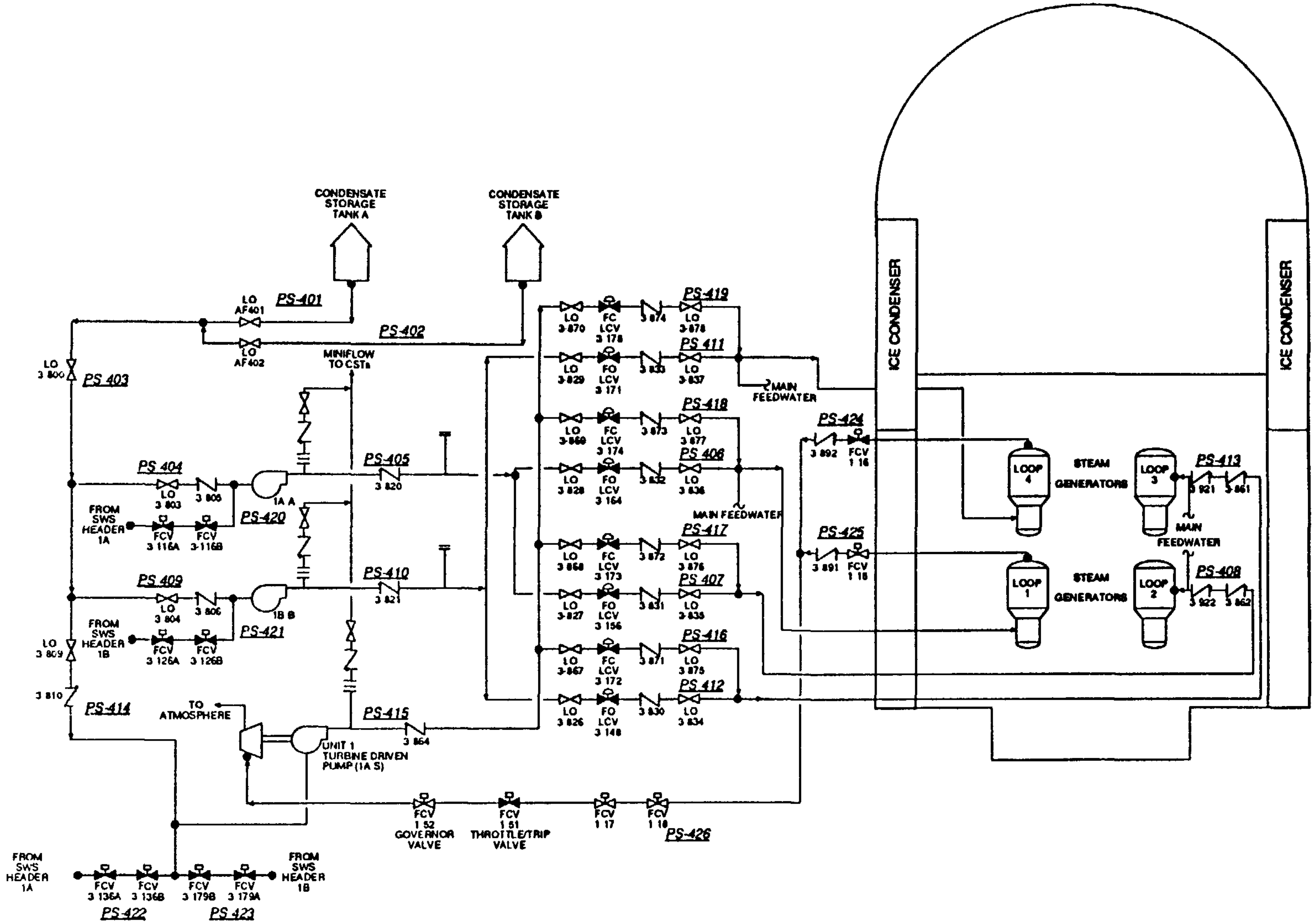


FIG. A2-1. Simplified schematic of the auxiliary feedwater system.

The charging system is described in case study 1. On loss of main feedwater, high pressure injection is only required if a reactor coolant system leak develops (or letdown is not isolated) or AFW is not available. Use of the safety injection system would require depressurization of the reactor to 1400 psig. If AFW was not available operator action would be required to implement feed and bleed for adequate core cooling.

Both the CCP A pump and AFW B pump were in a maintenance outage for surveillance activities at the time of the incident. The precise physical state of each component is not known, but both surveillance activities (SI-40.1 and SI-298.2) are known to be of relatively short duration (one-half to 2 hours) and do not involve disassembly of components. Restoration of the trains to operable status would require repositioning of some valves and racking in circuit breakers. Therefore, it is believed that these components could have been restored to service in about 15 minutes to one-half hour. Also note that with CCP A out of service CCP B would be running.

Incident Modeling

This incident has been modeled as a loss-of-feedwater transient with the A train CCP and B train AFW/MDP unavailable due to test and maintenance. The potential accident sequences associated with the incident are found on the T_2 event tree. AFW (L_1), and high pressure injection (D_1, D_3) functions are potentially affected. The sequences which are potentially affected by the incident have been identified in Figure A2-2.

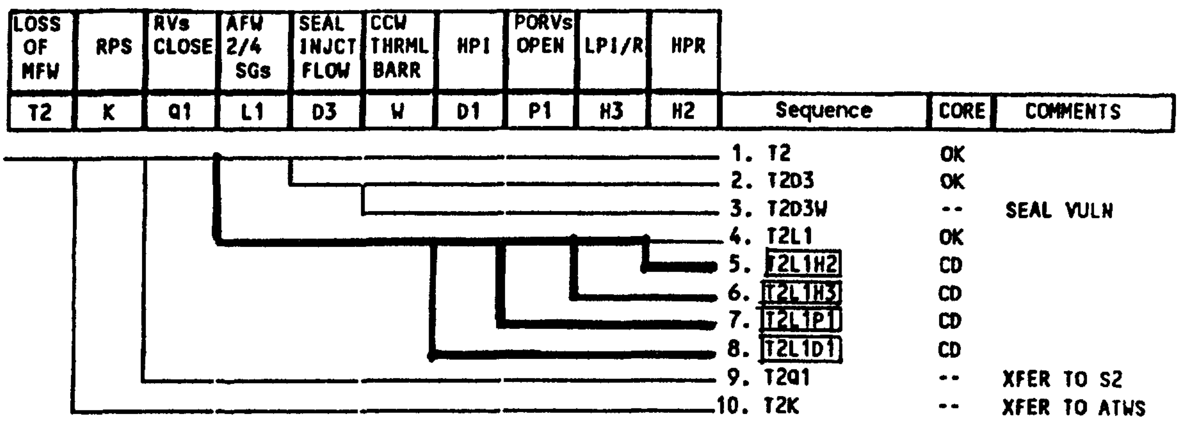


FIG. A2-2. Event tree for T_2 — loss of main feedwater.

The basic events which are affected by the incident and their associated probabilities are provided in Table A2-2. Note that test and maintenance contributions from the operating charging system and AFW system trains were disallowed to conform to operation and technical specification constraints, because CCP 2A-A was out of service, CCP 2B-B was operating. Therefore, no failure to start probability was applied to CCP 2B-B.

TABLE A2-2

BASIC EVENT/INITIATING EVENT PROBABILITIES

Event	PSA	Incident
IE-T2 loss of MFW	.72/yr	1.0
AFW-MDP-TM-2BB AFW pump 2B-B unavail due to T/M	2×10^{-3}	house event (1.0)
CHP-MDP-TM-2AA charging pump 2A-A unavail due to T/M	2×10^{-3}	house event (1.0)
AFW-MDP-TM-2AA FW pump 2A-A unavailable due to T/M	2×10^{-3}	0
AFW-TDP-TM-1AS AFW TDP unavailable due to T/M	1×10^{-2}	0
NREC-AFW-MDP-2BB non-recovery of AFW pump 2B-B	-	10^{-2} (range of 3×10^{-2} to 8×10^{-4})
NREC-CHP-MDP-2AA non recovery of CCP 2A-A	-	10^{-2} (range of 3×10^{-2} to 8×10^{-4})

Recovery of AFW pump 2B-B and CCP 2A-A was considered as a possibility with the constraint that either one must be made operable within about one-half to one hour after a loss of all heat removal capability. Main feedwater recovery (partial) may also have been possible. However, in light of the system malfunctions reported, no credit was given for MFW recovery. Recovery probabilities for CCP 2A-A and AFW MDP 2B-B were derived assuming operator actions were limited to valve and/or circuit breaker manipulations, did not require any complicated diagnostic actions, and were generally well covered by procedures and training. As a result, the recovery actions are thought to be bounded by groups 4 and 11 of NUREG/CR-4834 [6] at about 60 minutes. Recovery was assumed possible for any one but not both of these pumps for any given sequence.

Analysis Results

The conditional core damage probability associated with the incident is on the order of 1.8×10^{-6} with credit given for recovering either an AFW or charging pump. Prior to crediting any recovery the conditional core damage probability was about 6×10^{-5}. This result suggests that recovery actions have an important role in reducing the potential risks associated with this incident. The results for sequences involving this incident are provided in Table A2-3. These accident sequences primarily involve failure of the operable AFW trains (1A-A and 1AS) and failure of feed and bleed.

TABLE A2-3

SEQUENCE CONDITIONAL PROBABILITY RESULTS

Sequence	without recovery	with recovery
$T_2\ L_1\ H_2$	1.5×10^{-5}	1.5×10^{-7}
$T_2\ L_1\ H_3$	1.4×10^{-6}	1.4×10^{-8}
$T_2\ L_1\ P_1$	4.8×10^{-5}	1.6×10^{-6}
$T_2\ L_1\ D_1$	1.3×10^{-8}	1.3×10^{-8}
Total	6.5×10^{-5}	1.8×10^{-6}

Interestingly, sequences which include AFW and high pressure injection failure were found to be relatively unlikely even given the initial conditions. This is primarily due to redundancy and some diversity in the HPI function (safety injection was available, if the operators would depressurize the reactor). Thus, common cause hardware failures and operator actions (failure to properly initiate feed and bleed) are the major contributors.

The fact that there was a simultaneous maintenance outage of a charging system and AFW train ongoing was mitigated by the nature of the outage (i.e. surveillance vs. maintenance) and the fact that these trains could have been restored to service promptly and easily.

There is, however, an impact associated with AFW and charging system simultaneous unavailability that surfaced. In this state of operation, AFW system reliability is moderately reduced while charging system reliability is also reduced. The potential for reliance on safety injection increases, and operator action to reduce reactor pressure by opening PORVs and/or using pressurizer sprays becomes quite important. Thus, basic events and operator actions related to the available AFW trains and implementation of feed and bleed have the highest calculated importances (Fussell-Vesely, risk reduction). The AFW system has by far the highest risk increase importance suggesting that any further degradations in availability of either the turbine-driven train (most important) or motor-driven pump train A could have had a substantial risk impact.

NRC Form 366 (9-83) U.S. NUCLEAR REGULATORY COMMISSION APPROVED OMB NO. 3150-0104 EXPIRES 8/31/88

209818

LICENSEE EVENT REPORT (LER) JUL 25 1988 W.

FACILITY NAME (1)	DOCKET NUMBER (2)	PAGE (3)
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	1 OF 0 6

TITLE (4) Reactor Trip On Steam/Feedwater Flow Mismatch Coincident With Low Steam Generator Level Due To Plugged Sight Glass

EVENT DATE (5) MONTH	DAY	YEAR	LER NUMBER (6) YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	REPORT DATE (7) MONTH	DAY	YEAR	OTHER FACILITIES INVOLVED (8) FACILITY NAMES	DOCKET NUMBER(S)
0 5	1 9	8 8	8 8	0 2 3	0 1	0 7	0 7	8 8		0 5 0 0 0
										0 5 0 0 0

Rev. 0 on file

THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10 CFR §: (Check one or more of the following) (11)

OPERATING MODE (9): 1

POWER LEVEL (10): 0 7 2

[XX] 50.73(a)(2)(i)

LICENSEE CONTACT FOR THIS LER (12)

NAME	TELEPHONE NUMBER
K. E. Meade, Plant Operations Review Staff	AREA CODE 6 1 5 — 8 7 0 - 6 2 5 0

COMPLETE ONE LINE FOR EACH COMPONENT FAILURE DESCRIBED IN THIS REPORT (13)

CAUSE	SYSTEM	COMPONENT	MANUFACTURER	REPORTABLE TO NPRDS	CAUSE	SYSTEM	COMPONENT	MANUFACTURER	REPORTABLE TO NPRDS

SUPPLEMENTAL REPORT EXPECTED (14)

[ ] YES (If yes, complete EXPECTED SUBMISSION DATE) [XX] NO

EXPECTED SUBMISSION DATE (15) MONTH DAY YEAR

ABSTRACT (Limit to 1400 spaces, i.e., approximately fifteen single-space typewritten lines) (16)

This LER is being revised to update the corrective action section of this report. On May 19, 1988, with unit 2 at 71.7 percent reactor power, a reactor trip occurred at 1413 EDT. At 1350 EDT, a senior reactor operator (SRO) and an instrument mechanic (IM) started the process of making adjustments to the No. 3 heater drain tank (HDT) level controllers. The SRO and IM proceeded to troubleshoot the problem in an attempt to reduce the level in the subject tank. After three or four manipulations, the SRO noted the HDT pumps began to cavitate, and a subsequent trip of the pumps occurred. At 1405 EDT, the balance of plant (BOP) operator noted fluctuations in the No. 3 HDT discharge flow. At 1408 EDT, both No. 3 HDT pumps tripped. The BOP started a reduction in turbine load. At this time it was noted that steam generator (S/G) No.1 level was dropping. The operator took manual control of the feedwater regulator valve and went to full open to regain level. Level dropped to 21 percent in the No. 1 S/G before level turned around and started to ascend. The "A" main feedwater pump backed off in speed as it was in the automatic control. However, "B" main feedwater pump continued in manual control causing feedwater flows to be high. Level continued to increase to 60 percent at which point the regulator valves automatically closed as designed. This resulted in a steam/feedwater flow mismatch. The S/G loop 3 low level bistable was already tripped as a result of 2-LT-3-97 being out of service. Therefore, a reactor trip signal was generated due to a steam/feedwater flow mismatch coincident with low S/G level in loop 3. The mismatch was caused by a S/G level transient induced by a manual BOP runback as a result of No. 3 HDT level manipulation and subsequent loss of the No. 3 HDT pump. The low S/G level was caused by bistable 2-LS-3-97 being in the tripped condition due to environmental qualification concerns. The trip was reviewed with Operations personnel to ensure familiarization with the event and to detail the lessons that could be learned from the transient.

NRC Form 366A (9-83)

U.S. NUCLEAR REGULATORY COMMISSION

APPROVED OMB NO 3150-0104 EXPIRES 8/31/88

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6) YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	PAGE (3)
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	8 8	— 0 2 3	— 0 1	0 2 OF 0 6

TEXT (If more space is required, use additional NRC Form 366A's) (17)

This LER is being revised to update the corrective action section of this report.

DESCRIPTION OF EVENT

On May 19, 1988, with unit 2 at 71.7 percent reactor power (2235 psig and 566 degrees F), a reactor trip occurred at 1413 EDT. The trip was the result of a steam flow/feedwater flow mismatch coincident with a low steam generator (S/G) level in loop 3.

Prior to the event the following initial conditions existed:

1) Control rods were in manual
2) "A" main feedwater pump was in automatic
3) "B" main feedwater pump was in manual control
4) "A" & "B" No. 3 Heater Drain Tank (HDT) operating
5) 2AA centrifugal charging pump was inoperable for SI-40.1
6) 2BB AFW pump inoperable for SI-298.2
7) 2-LT-3-97 (S/G level loop 3) inoperable due to EQ concerns (all bistables tripped)

At approximately 1350 EDT, a senior reactor operator (SRO) and an instrument mechanic (IM) started the process of making adjustments to the No. 3 HDT level controllers. The SRO had been told by the Turbine Building assistant unit operator (AUO) that the No. 3 HDT level was high as noted by visual observation of the sight glass. It was also noted that the controller was set at zero. Using WR B253109, the SRO and IM proceeded to troubleshoot the problem in an attempt to reduce the level in the subject tank. This was being done by a series of small incremental adjustments to the controller followed by checks of the sight glass level, HDT discharge valve position, and HDT pump suction pressure. After the third or fourth such manipulation with no resultant changes in sight glass level, the SRO noted the HDT pumps began to cavitate, and a subsequent trip of the pumps occurred.

At approximately 1405 EDT, the balance of plant (BOP) operator noted fluctuations in the No. 3 HDT discharge flow and subsequent perturbations in the No. 3 HDT pump amperages. Also, the hotwell level was increasing and flow was oscillating. The operator notified the lead operator and the assistant shift operation supervisor (ASOS). At approximately 1408 EDT, both No. 3 HDT pumps tripped (motor trip out alarm received). The BOP immediately started a reduction in turbine load using the governor valve positioner at the rate of three percent per minute. Recognizing a further reduction was required, the BOP went to valve position limiter control and continued to reduce power. The lead operator had placed the rods in automatic, and the rods stepped in on Tave/Tref mismatch. At this time it was noted that S/G No.1 level was dropping. The operator took manual control of feedwater regulator valve 2-FCV-3-35 (loop 1) and went to full open to regain level. The operator also opened the bypass regulator valve to 20 percent for additional feedwater flow. Level dropped to 21 percent in the No. 1 S/G before level turned around and started to ascend.

NRC Form 366A (9-83)

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

U.S. NUCLEAR REGULATORY COMMISSION
APPROVED OMB NO. 3150-0104
EXPIRES 8/31/88

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6) YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	PAGE (3)
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	8 8	— 0 2 3 —	0 1	0 3 OF 0 6

TEXT (If more space is required, use additional NRC Form 366A's) (17)

The "A" main feedwater pump backed off in speed as it was in the automatic control. However, "B" main feedwater pump continued in manual control causing feedwater flows to be high. The operator took manual control of loops 2, 3, and 4 regulator valves and closed down on the valves to reduce feedwater flow to loops 2, 3, and 4. Level continued to increase to 60 percent at which point the regulator valves automatically closed as designed. This resulted in a steam flow/feedwater flow mismatch as the feedwater flow had decreased. Since the S/G loop 3 low level bistable was already tripped as a result of 2-LT-3-97 being out of service, a reactor trip occurred.

The lead operator announced the reactor trip and proceeded to enter E-0, "Reactor Trip or Safety Injection - Units 1 and 2." The ASOS pulled the procedure and had the operators verify the appropriate actions. Following the reactor trip, pressurizer pressure decreased to 1970 psig and pressurizer level decreased to approximately 10 percent. A letdown isolation occurred as a result of the low pressurizer level. The pressurizer pressure and level decrease was due to the cooldown of the reactor coolant system (RCS); however, the RCS and pressurizer cooldown limits specified in TS were not exceeded. Reactor coolant temperature (Tave) in loop 1 decreased to approximately 500 degrees F and to 521 degrees F in the other loops. Loop 1 was lower because the AFW turbine-driven pump was being supplied from this loop. In addition to the reactor trip, the cooldown was exacerbated by steam leaking through the "A" MFPT throttle valve and an intermittent opening of a steam dump valve to the condenser, FCV-1-104. The rod bottom light for shutdown bank "D" rod E-13 did not illuminate; however, the operator verified that the rod position indicator was at zero. It was determined that the rod bottom light had burnt out and that the rod was in the correct position. The light bulb was subsequently replaced. Anomalies noted were:

1) The steam dump valve 2-FCV-1-104 intermittently opened without demand.
2) The "A" main feedwater pump steam valves leaked through causing approximately 2000 RPM.
3) Loop 1 feedwater regulator valve failed to respond in automatic.
4) Hotwell level decreased following the trip such that it appeared that the vacuum drag valve from the condensate storage tank was slow or did not respond to the transient.

However, none of the above anomalies affected the response nor the recovery from the reactor trip. Recovery of the trip was initiated using ES-0.1, "Reactor Trip Response, Units 1 & 2."

NRC Form 366A (9-83)

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

U.S. NUCLEAR REGULATORY COMMISSION
APPROVED OMB NO. 3150-0104
EXPIRES 8/31/85

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6)			PAGE (3)
		YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	8 8	— 0 2 3	— 0 1	0 4 OF 0 6

TEXT (If more space is required, use additional NRC Form 366A's) (17)

CAUSE OF EVENT

The reactor trip was the result of a steam/feedwater flow mismatch coincident with low S/G level in loop 3. The steam/feedwater flow mismatch was caused by a S/G transient induced by a manual BOP runback as a result of No. 3 HDT level controller manipulation and subsequent loss of No. 3 HDT pump. The SRO was manipulating the level controller because the sight glass on the tank was reading high. The sight glass was later found to be plugged and thus giving a false indication. The low S/G level was caused by bistable 2-LS-3-97 being in the tripped condition due to environmental qualification concerns. A splice was found on 2-LT-3-97 which was believed to not be environmentally qualified as required by 10 CFR 50.49. This problem is detailed in LER SQRO-50-328/88022.

ANALYSIS OF EVENT

This report is being submitted under the requirements of 10 CFR 50.73, paragraph a.2.iv, as an event which resulted in the automatic actuation of an engineered safety feature.

The safety-related equipment required to mitigate the transient operated as designed. The SSPS logic was completed with the reactor trip breakers opening and subsequently all rods on the bottom. A feedwater isolation occurred on the reactor trip coincident with a low Tave. Letdown isolated at 17 percent pressurizer level. No PORVs or safety valves lifted. The available AFW pumps started as designed, and the turbine tripped on the reactor trip as required.

Operations personnel performance during the transient demonstrated a thorough knowledge of system performance and the ability to reset and control plant transients.

CORRECTIVE ACTIONS

The following corrective actions were completed before the plant reentered mode 2:

1. The No. 1 regulator valve failed in the as-is position. This valve has been repaired.

2. 2-FCV-1-104 inadvertently opened during the transient. The valve controllers were checked and repaired.

3. 2-LCV-3-97 was repaired with the proper EQ splice

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6) YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	PAGE (3)
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	8 8	— 0 2 3	— 0 1	0 5 OF 0 6

TEXT (If more space is required, use additional NRC Form 366A's) (17)

The following corrective actions were completed before the plant entered mode 1.

1. The sight glass on the No. 3 HDT was cleaned and verified to be working properly.

2. The controllers on No. 3 HDT were recalibrated.

3. Valves 2-LCV-6-106 A&B and 2-LCV-6-105 A&B have been verified to stroke properly from the controllers.

4. The No. 3 HDT motor trip out light was repaired.

5. Operators and System Engineering were interviewed to determine if any sight glass on feedwater heaters, hotwell, and No. 7 HDT have indications of potential blockage which might result in false level indications. All necessary repairs were accomplished.

6. The vacuum drag valve to the condenser (2-LCV-2-9) was troubleshot and repaired as necessary.

The trip was reviewed with Operations personnel to ensure familiarization with the event and detail the lessons that could be learned from the transient.

Other corrective actions for the event are as follows:

1. Review SQM-2 to determine if further clarification is required for use of generic WRs, such as the one used to manipulate No. 3 HDT level. Revise this procedure if required and provide a SQN dispatch to describe plant policy. This action will be completed by June 20, 1988.

2. Research in-plant versus control room communication for operational necessities/emergencies. Consider dedicated phone line to each horseshoe. This action will be completed by June 30, 1988.

3. Implement a formalized troubleshooting procedure outlining the guidelines on types of troubleshooting allowed and when it is allowed. This action will be completed by July 30, 1988.

4. The main feedwater pump (MFP) high and low pressure stop valves and high pressure governor valves will be repaired, if necessary, before startup following the next unit 2 refueling outage (WR B751430 on the 2A MFP and WR B751429 on 2B MFP).

NRC Form 366A (9-83)

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

U.S. NUCLEAR REGULATORY COMMISSION
APPROVED OMB NO 3150-0104
EXPIRES: 8/31/88

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6) YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	PAGE (3)
Sequoyah, Unit 2	0 5 0 0 0 3 2 8	8 8	— 0 2 3	— 0 1	0 6 OF 0 6

TEXT (If more space is required, use additional NRC Form 366A's) (17)

COMMITMENTS

1. Review SQM-2 to determine if further clarification is required for use of generic WRs. Revise this procedure if required and provide a SQN dispatch to describe plant policy. This action will be completed by June 20, 1988.

2. Research in-plant versus control room communication for operational necessities/emergencies. Consider dedicated phone line to each horseshoe. This action will be completed by June 30, 1988.

3. Implement a formalized troubleshooting procedure outlining the guidelines on types of troubleshooting allowed and when it is allowed. This action will be completed by July 30, 1988.

4. The main feedwater pump (MFP) high and low pressure stop valves and high pressure governor valves will be repaired, if necessary, before startup following the next unit 2 refueling outage (WR B751430 on the 2A MFP and WR B751429 on 2B MFP).

098SQ

CASE STUDY 3

INOPERABLE POWER OPERATED RELIEF VALVES

Surry Unit 1 (15 April 1988)
LER 280/88-011

Description

At 0505 on April 15 1988, Surry 1 was in cold shutdown with the reactor coolant temperature at $130^{\circ}F$ and pressure at 40 psi. When the RCS temperature is below $350^{\circ}F$, Technical Specifications require that both power-operated relief valves (PORVs) be operational to provide relief capability to minimize pressure transients. During routine RCS depressurization operations, PORVs PCV-1455C and PVC-1456 failed to manually open when operators tested the valves. The operators unsuccessfully attempted to open both PORVs from their respective control room three-position selector switches by turning each switch from the AUTO to the OPEN position. Both valves were later opened by turning their switches from the CLOSE to the OPEN position. Upon failure of the valves, both valves were declared inoperable and left open per the plant Technical Specifications.

Table A3-1 provides a summary of the chronology of this incident. The incident is more fully described in LER 280/88-011 attached to the end of this case study.

Plant Design and Operational Considerations

Two PORVs are provided on Surry Unit 1. The arrangement of these valves and their block valves is shown in Figure A3-1. The PORVs are designed to lift prior to the safety valves, thereby reducing the number of challenges to the unisolable safety valves. In the PSA, the PORVs are required to operate properly for pressure relief, close properly for Reactor Coolant System (RCS) integrity and operate on demand for the feed and bleed cooling mode for decay heat removal.

Feed and bleed cooling is relied on whenever secondary cooling (main feedwater and auxiliary feedwater) is not available and decay heat is not being removed by sufficient energy loss from the RCS (large and medium loss-of-coolant-accidents).

TABLE A3-1

INCIDENT CHRONOLOGY, EQUIPMENT FAILURES AND OPERATOR ACTIONS

Initial Conditions

Reactor at cold shutdown, 40 psi , 130^{o}F

Normal depressurization evolution in progress

Chronology

Depressurization evolution in progress

Operator attempted to open both PORVs, both failed to open

PORVs were opened by taking the 3-way switches to CLOSE and then to OPEN

PORVs were declared inoperable and left open in accordance with the Technical Specifications

Operator Actions

Operators conducting routine depressurization

Manual opening of PORVs failed

Recovery of failed PORVs

Equipment Failures

PORVs 1433C and 1456 failed to open on demand

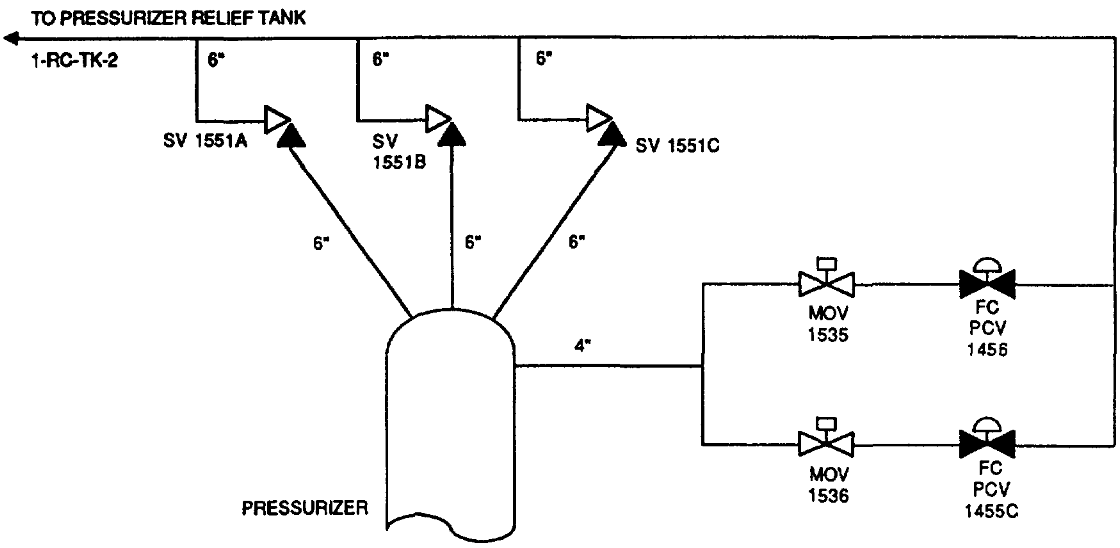


FIG. A3-1. Simplified sketch of PPRS system.

Incident Modeling

This incident has been modeled for transients as the loss of feed and bleed capability due to the inability of the plant operators to open the PORVs. For the ATWS events, this incident has been modeled as a reduced capability to provide RCS pressure relief (the safety relief valves are still available). It is assumed that the problem would have existed during the full operating cycle with the plant at power and would not normally be detected except in a refueling outage during PORV operational testing. An exposure time of one year was used in the analysis.

The potential accident sequences associated with this incident are found on each transient event tree (except station blackout), on the small and very small LOCA event trees, and on the ATWS event tree. Figures A3-2 through A3-8 show these sequences. The event tree top events of concern are P, P1 and P2. Top events P and P1 are associated with the establishment of feed and bleed cooling and contain only basic events pertaining to the PORVs and their block valves. This incident renders these top events failed. Top event P2 is associated with RCS pressure relief during ATWS and contains safety relief valves as well as PORVs. This top event is reduced in reliability by this incident since operator diagnosis and corrective action would be required given the conditions that existed with the PORVs.

Although the operators were able to eventually get the PORVs open in this instance, no information was provided on how long it took them to do so. It is presumed that some time lapsed. It is believed that such a recovery is possible with the plant at power during an incident requiring feed and bleed cooling. However, due to more severe timing constraints, stress levels, and harsh equipment environment, the likelihood of failing to make such a recovery seems high. For loss-of-coolant accidents and ATWS sequences no attempt was made to conduct the analysis needed to derive a meaningful recovery factor. Therefore, no recovery was applied to these sequences.

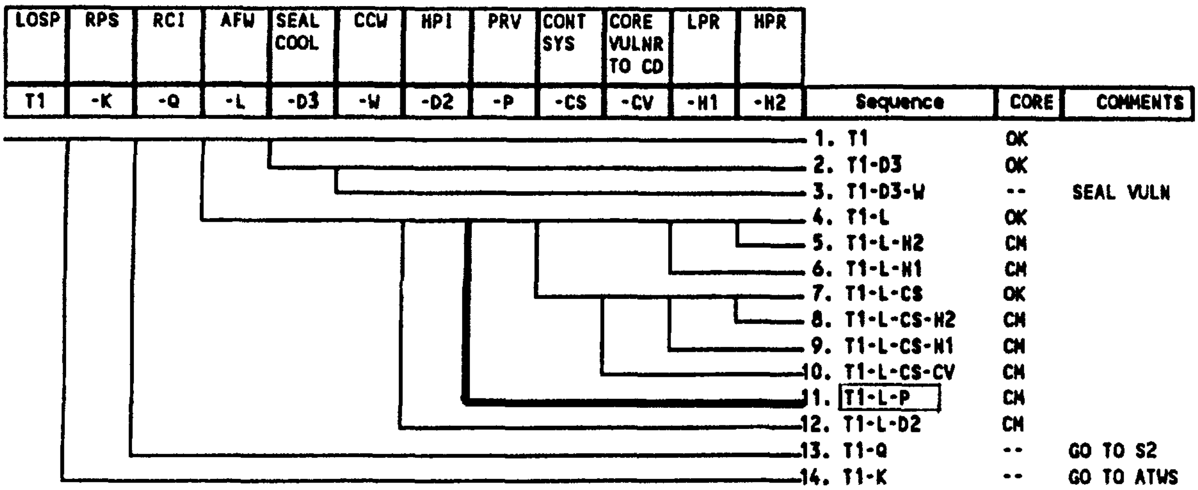


FIG. A3-2. Event tree for T_1 — loss of offsite power.

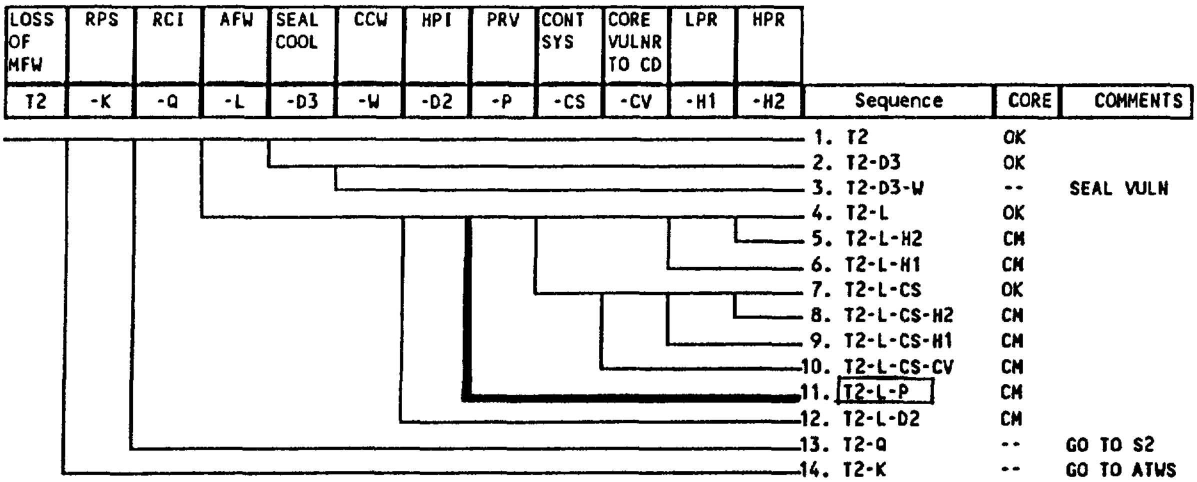


FIG. A3-3. Event tree for T_2 — loss of main feedwater.

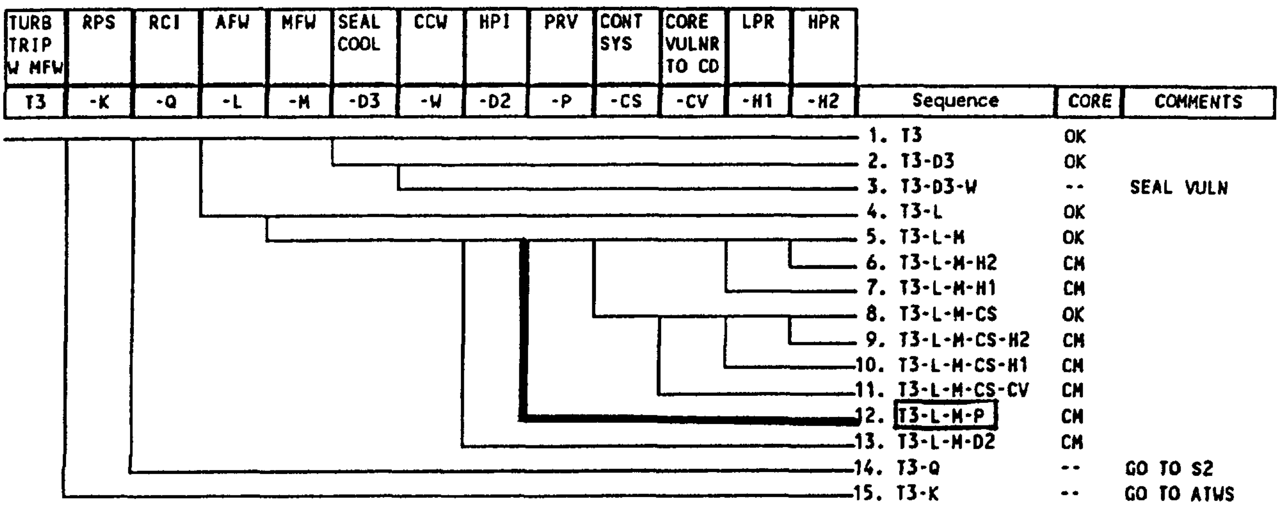


FIG. A3-4. Event tree for T_3 — turbine trip with MFW.

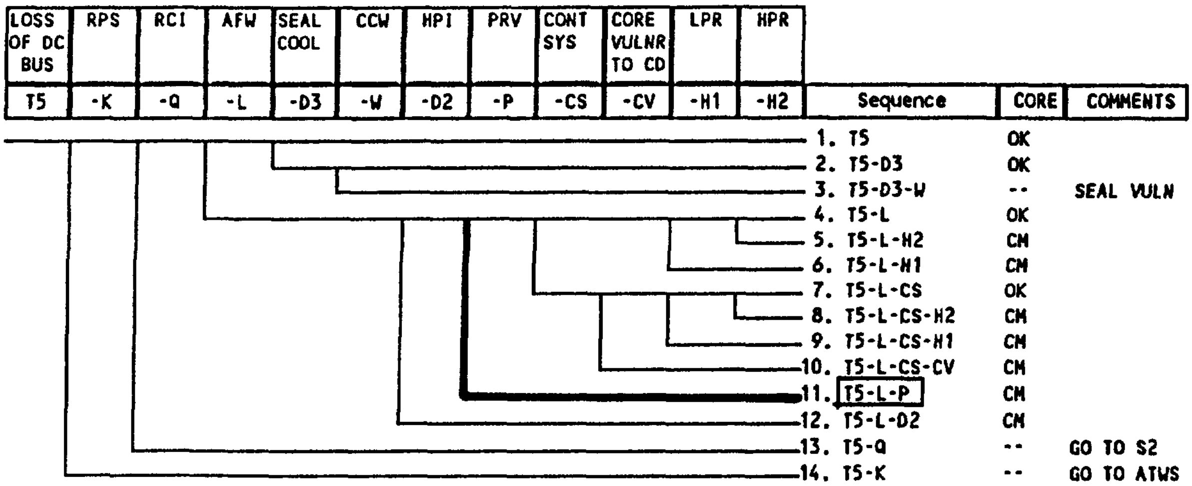


FIG. A3-5. Event tree for T_5 — loss of DC bus.

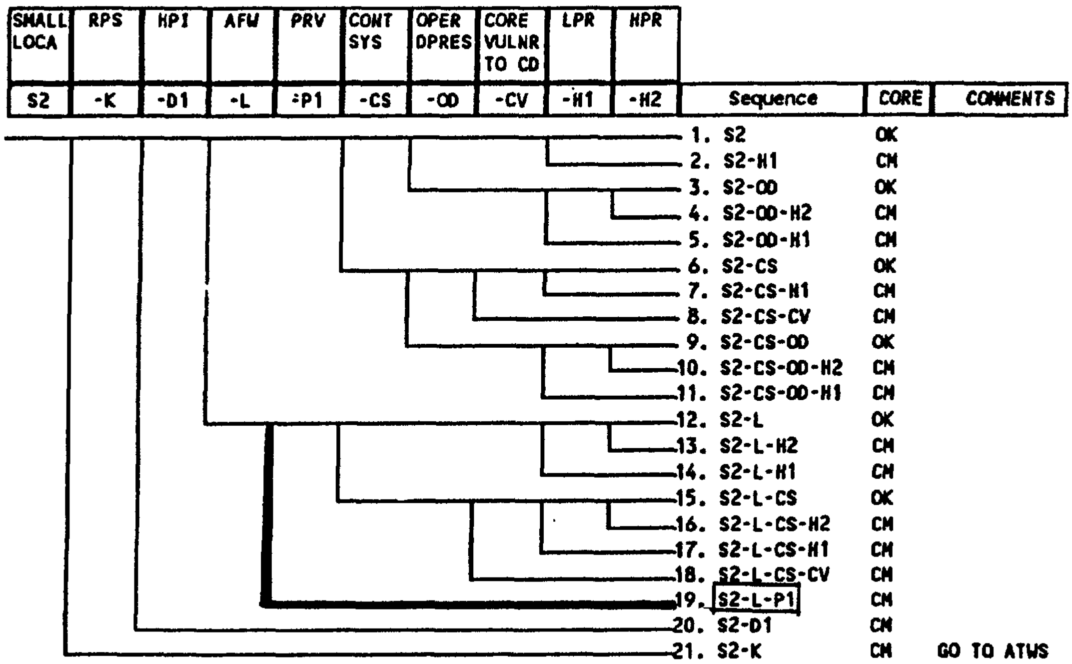


FIG. A3-6. Event tree for S_2 — small LOCA.

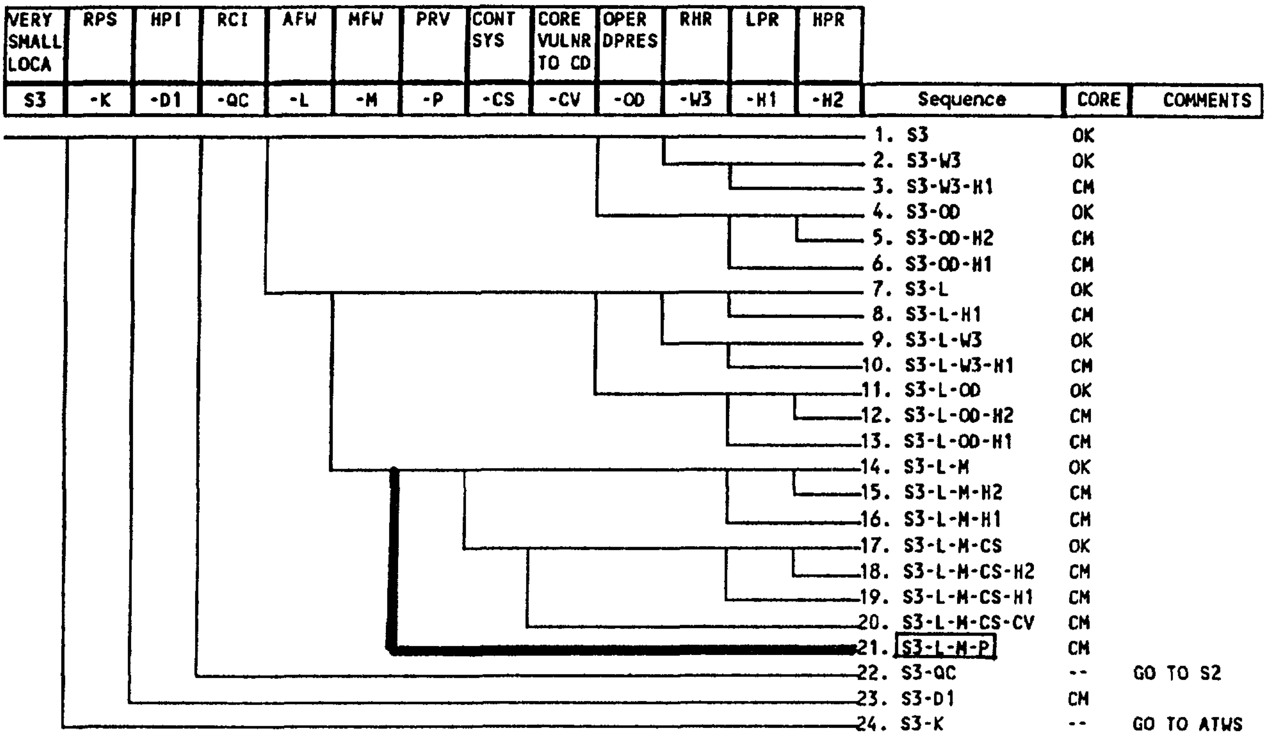


FIG. A3-7. Event tree for S_3 — very small LOCA.

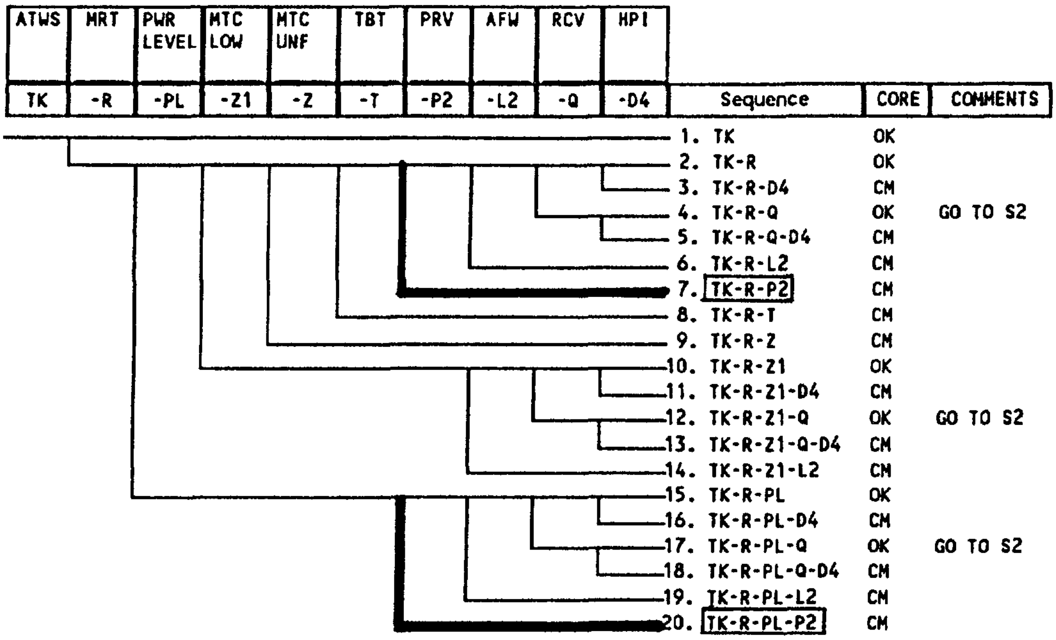


FIG. A3-8. Event tree for T_k — anticipated transient without scram.

Table A3-2 provides a list of the basic events and the changes made. The recovery action for the initiation of feed and bleed cooling is based on the upper 95% confidence limit for recovery action group 3 at 60 minutes from NUREG/CR-4834 [6]. A sensitivity was performed using the mean value for the same distribution.

TABLE A3-2

BASIC EVENT/RECOVERY ACTION PROBABILITIES

Event	PSA	Incident
PPS-CCF-FT-PORV common cause failure of the PORVs to open	7.0×10^{-5}	house event (1.0)
PPS-SOV-FT-1455C PORV 1455C fails to open on demand	1.0×10^{-3}	house event (1.0)
PPS-SOV-FT-1456 PORV 1456 fails to open on demand	1.0×10^{-3}	house event (1.0)
NREC-PORV Non-recovery of PORVs failing to open	-	0.042
NREC-PORV2 Non-recovery of PORVs failing to open (sensitivity case)	-	0.0011

Analysis Results

The conditional core damage probability associated with this incident is about 1.4×10^{-5} with credit given for recovery of both PORVs within one hour (excluding ATWS and LOCA sequences). Prior to any recovery the conditional core damage probability was about 3.2×10^{-4}. This result suggests that recovery actions have a very important role in reducing the potential risks associated with this incident. The results for sequences involving this incident are shown in Table A3-3. The dominant sequence involves a transient initiated by a loss of main feedwater and failure of auxiliary feedwater, thereby causing a demand for feed and bleed cooling that can not be met due to the PORV failures. This accounts for about 85% of the conditional core damage probability. The next highest contributor is a loss of offsite power transient with failure of the auxiliary feedwater system. Emergency power is supplied by the diesel generators, thus feed and bleed cooling would have been possible if the PORVs were available.

TABLE A3-3

SEQUENCE CONDITIONAL PROBABILITIES

Sequence	Without recovery	With recovery (0.042)	Recovery Sensitivity (0.0011)
T_1 L P	2.3×10^{-5}	9.7×10^{-7}	2.5×10^{-8}
T_2 L P	2.8×10^{-4}	1.2×10^{-5}	3.1×10^{-7}
T_3 L M P	6.3×10^{-6}	2.6×10^{-7}	6.9×10^{-9}
T_5 L P	3.0×10^{-6}	1.3×10^{-7}	3.3×10^{-9}
S_2 L P_1	3.0×10^{-7}	3.0×10^{-7}	3.0×10^{-7}
S_3 L M P	5.0×10^{-7}	5.0×10^{-7}	5.0×10^{-7}
T_k R P_2	1.8×10^{-7}	1.8×10^{-7}	1.8×10^{-7}
T_k R PL P2	1.8×10^{-8}	1.8×10^{-8}	1.8×10^{-8}
Total	3.2×10^{-4}	1.4×10^{-5}	1.3×10^{-6}

The dominant component failures involve common cause failures and recovery actions for the auxiliary feedwater system. The auxiliary feedwater system is critical to the safe operation of the plant as it is the only remaining safety related means of removing decay heat in an accident scenario. Thus, steam binding of the pumps, common cause failure of the AFW pumps to start, and failure to cross-connect AFW to the other unit dominate failure of the AFW system and the conditional core damage probability.

After the AFW system, the main feedwater system is the next most important function to have available. MFW is not possible in loss of offsite power events and events where loss of MFW is the initiator.

From the perspective of what is now key to preventing further increase in the conditional core damage probability, items that prevent further degradation of the AFW system are important. Low failure rate items such as condensate storage tank failure and key check valve failures can now dramatically increase the conditional core damage probability should they fail.

NRC Form 366 (9-83) U.S. NUCLEAR REGULATORY COMMISSION
APPROVED OMB NO 3150-0104
EXPIRES 8/31/88

LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)	DOCKET NUMBER (2)	PAGE (3)
Surry Power Station, Unit 1	0 5 0 0 0 2 8 0	1 OF 0 3

TITLE (4): Inoperable PORVs Due To Inadequate Procedure

EVENT DATE (5) Month	Day	Year	LER NUMBER (6) Year	Sequential Number	Revision Number	REPORT DATE (7) Month	Day	Year	OTHER FACILITIES INVOLVED (8) Facility Names	Docket Number(s)
0 4	1 5	8 8	8 8	0 1 1	0 1	0 8	2 6	8 8		0 5 0 0 0
										0 5 0 0 0

OPERATING MODE (9): N
POWER LEVEL (10): 0 0 0

THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10 CFR §: (Check one or more of the following) (11)

- [ ] 20.402(b)
- [ ] 20.405(a)(1)(i)
- [ ] 20.405(a)(1)(ii)
- [ ] 20.405(a)(1)(iii)
- [ ] 20.405(a)(1)(iv)
- [ ] 20.405(a)(1)(v)
- [ ] 20.405(c)
- [ ] 50.36(c)(1)
- [ ] 50.36(c)(2)
- [ ] 50.73(a)(2)(i)
- [ ] 50.73(a)(2)(ii)
- [ ] 50.73(a)(2)(iii)
- [ ] 50.73(a)(2)(iv)
- [x] 50.73(a)(2)(v)
- [ ] 50.73(a)(2)(vii)
- [ ] 50.73(a)(2)(viii)(A)
- [ ] 50.73(a)(2)(viii)(B)
- [ ] 50.73(a)(2)(x)
- [ ] 73.71(b)
- [ ] 73.71(c)
- [ ] OTHER (Specify in Abstract below and in Text, NRC Form 366A)

LICENSEE CONTACT FOR THIS LER (12)

NAME	TELEPHONE NUMBER
D. L. Benson, Station Manager	8 0 4 357-3184

COMPLETE ONE LINE FOR EACH COMPONENT FAILURE DESCRIBED IN THIS REPORT (13)

CAUSE	SYSTEM	COMPONENT	MANUFACTURER	REPORTABLE TO NPRDS	CAUSE	SYSTEM	COMPONENT	MANUFACTURER	REPORTABLE TO NPRDS
F	R C	V A L V	C 6 3 5	Y					

SUPPLEMENTAL REPORT EXPECTED (14)

- [ ] YES (If yes, complete EXPECTED SUBMISSION DATE)
- [x] NO

EXPECTED SUBMISSION DATE (15): Month | Day | Year

ABSTRACT (Limit to 1400 spaces, i.e. approximately fifteen single-space typewritten lines) (16)

On April 15, 1988 at 0505 hours, Unit 1 was at cold shutdown with reactor coolant temperature at 130 degrees Fahrenheit and pressure at 40 psig. During a normal depressurization evolution, both Power Operated Relief Valves (PORV) PCV-1455C and PCV-1456 failed to manually open when the respective three position (close-auto-open) selector switches were placed in the open position from the auto position. Both PORVs were later opened when the selector switches were placed in the open position from the closed position. These valves were declared inoperable and left open in accordance with Technical Specification T. S. 3.1.G. A four hour event notification was submitted in accordance with 10CFR50.72(b)(2)(iii)(D). This event is reportable pursuant to 10CFR50.73(a)(2)(v)(D).

After an extensive investigation, the cause of the PORV failure was determined to be a procedural inadequacy. The procedure failed to specify torque values for the diaphragm hold down screws and bolts. The improperly torqued bolts and screws allowed the actuator diaphragm to shift and resulted in intermittent PORV failure. The bolts and screws were properly torqued, and the PORVs were tested satisfactorily.

NRC Form 366A (9-83)
U.S. NUCLEAR REGULATORY COMMISSION
APPROVED OMB NO. 3150-0104
EXPIRES 8/31/88

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6) YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	PAGE (3)
Surry Power Station, Unit 1	0 5 0 0 0 2 8 0	8 8	— 0 1 1	— 0 1	0 2 OF 0 3

TEXT (If more space is required, use additional NRC Form 366A's) (17)

1.0 Description of the Event

On April 15, 1988 at 0505 hours, Unit 1 was at cold shutdown with reactor coolant temperature at 130 degrees Fahrenheit and pressure at 40 psig. During a normal depressurization evolution, both Power Operated Relief Valves (PORV EIIS-RV) PCV-1455C and PCV-1456 failed to manually open when the respective three position (close-auto-open) selector switches were placed in the open position from the auto position. Both PORVs were later opened when the selector switches were placed in the open position from the closed position. These valves were declared inoperable and left open in accordance with Technical Specification T. S. 3.1.G.

A four hour event notification was submitted in accordance with 10CFR50.72(b)(2)(iii)(D). This event is reportable pursuant to 10CFR50.73(a)(2)(v)(D).

2.0 Safety Consequences and Implications

When the reactor coolant average temperature is less than 350 degrees Fahrenheit and the reactor vessel head is bolted, the Technical Specifications require the operability of two PORVs or the Reactor Coolant System (RCS) be vented through an open PORV. This ensures that the reactor vessel will be protected from pressure transients which could exceed the limits of Appendix G of 10CFR50. When the reactor coolant average temperature is greater than 350 degrees Fahrenheit, overpressure protection is provided by a bubble in the pressurizer and/or pressurizer safety valves.

When the PORVs were determined to be inoperable, both were placed in the open position to provide a vent path for the RCS in accordance with T. S. 3.1.G. No RCS pressure transients occurred during the unit outage that would have required the response of these valves. Therefore, these events did not constitute an unreviewed safety question and the health and safety of the public were not affected.

LICENSEE EVENT REPORT (LER) TEXT CONTINUATION

U.S. NUCLEAR REGULATORY COMMISSION
APPROVED OMB NO. 3150-0104
EXPIRES 8/31/88

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6) YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	PAGE (3)
Surry Power Station, Unit 1	0 5 0 0 0 2 8 0	8 8	— 0 1 1 —	0 1	0 3 OF 0 3

TEXT (If more space is required, use additional NRC Form 366A's) (17)

3.0 Cause

After an extensive investigation, which included close examination of the valves' operator, SOVs, air supply, and position switches, the root cause of the PORV failure was determined to be a procedural inadequacy. The procedure failed to specify torque values for the diaphragm hold down screws and bolts. This condition allowed the actuator diaphragm to shift and cause intermittent PORV failure.

4.0 Immediate Corrective Action(s)

When the PORVs were determined to be inoperable, they were placed in the open position to provide a RCS vent path in compliance with T. S. 3.1.G.

5.0 Additional Corrective Action(s)

The valve actuator bolts and screws were torqued to the correct value.

6.0 Action(s) Taken to Prevent Recurrence

The torque values for actuator bolts and screws will be added to the maintenance procedure.

7 ; Similar Events

None.

8.0 Manufacturer/Model Number

Copes Vulcan/D-100-160-2 1/2".

REFERENCES

[1] NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, Rep. NUREG-1150, Second Draft for Peer Review, NRC, Washington D.C.,June 1989.

[2] J.W. MINARICK, et al., Precursors to Potential Severe Core Damage Accidents: 1988, A Status Report, Rep. NUREG/CR-4674, ORNL/NOAC-232, (Vols. 9 and 10), Martin Marietta Energy Systems, Inc., Oak Ridge National Laboratory; Science Applications International Corp.; and Professional Analysis, Inc.; NRC, Washington D.C., February 1990.

[3] R.C. BERTUCIO, et al., Analysis of Core Damage Frequency: Sequoyah Unit 1", Rep. NUREG/CR-4550, Vol. 5, Rev. 1, SAND86-2084, Sandia National Laboratories, NRC, Washington D.C., April 1990.

[4] R.C. BERTUCIO, et al., Analysis of Core Damage Frequency: Surry Unit 1, Rep. NUREG/CR-4550, Vol. 3, Rev., SAND86-2084, Sandia National Laboratories, NRC, Washington D.C., April 1990.

[5] K.D. RUSSELL, et al., Integrated Reliability and Risk Analysis System (IRRAS), Version 2.5 Reference Manual Rep. EGG-2613, Idaho National Engineering Laboratory, NRC, Washington D.C. (to be published).

[6] D.W. WHITEHEAD, Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP), Vol. 2: Application of the Data-Based Method, Rep. NUREG/CR-4834, SAND87-0179, Sandia National Laboratories, NRC, Washington D.C., December 1987.

CONTRIBUTORS TO DRAFTING AND REVIEW

Mr. P. W. Baranowsky	US Nuclear Regulatory Commission Washington, D.C. United States of America
Mr. M. B. Sattison	Idaho National Engineering Laboratory Idaho Falls, Idaho United States of America
Mr. V. Tolstykh	Scientific Secretary International Atomic Energy Agency
Mr. B. Tomic	Scientific Secretary International Atomic Energy Agency
Mr. J. van Daatselaar	International Atomic Energy Agency

Consultants Meeting

Vienna, Austria: 24-28 September 1990