DRAFT

South Texas PSA Review: Evaluation of Internal Event Accident Frequency Estimates and Containment Binning

Interim Report

January 23, 1990

Prepared by:
Timothy A. Wheeler
Teresa T. Sype
Sandia National Laboratories
Division 6412
P.O. Box 5800
Albuquerque, New Mexico 87185

John L. Darby, Bob Walsh
Science and Engineering Associates, Inc.
SEA Plaza
6100 Uptown Blvd. N.E., Suite 700
Albuquerque, New Mexico 87190

Foreword

The objective of this review is to evaluate the South Texas Project (STP) Probability Safety Analysis (PSA) for the USNRC. The PSA was reviewed for thoroughness of analysis, accuracy in plant modeling, legitimacy of assumptions, and overall quality of the work. The review is limited to the internal event analysis. A review of the fire accident analysis will be presented in a later report.

This review is not a pass/fail evaluation of the adequacy of the PSA. The adequacy of the analysis depends on the intended uses and must be addressed on a case-by-case basis by the licensee and the NRC. This review identifies strengths, weakness, and areas where additional clarification would assist the NRC in evaluating the PSA for specific regulatory purposes.

It should be noted that the licensee, Houston Lighting and Power, did not see any of the comments in this review prior to its release to the NRC. The licensee has not had the opportunity to respond to any statement made or question raised by this interim report. Some of the concerns raised by this review will undoubtedly be resolved after further communication with the licensee.

1.0 INTRODUCTION

This report summarizes a review of the South Texas Project (STP) Probabilistic Safety Assessment (PSA).[1] The PSA was produced by Houston Lighting and Power Company (HLP) using the services of Pickard, Lowe, and Garrick, Inc. (PLG).

The review was conducted by Sandia National Laboratories (SNL) with assistance from Science and Engineering Associates, Inc. (SEA). This report focuses on internal initiating events only.

The May 1989 version of the PSA was reviewed. Other material utilized in the review included: An up-to-date Final Safety Analysis Report (FSAR),[2] System Descriptions as included in the PSA, numerous Piping and Instrumentation Diagrams (P&IDs), logic diagrams, elementary wiring diagrams, technical specifications, and emergency operating procedures (EOP). A two-day site visit in November, 1989 supplemented this written material.

In Section 2 the assumptions regarding the plant systems which were incorporated into the PSA are discussed. This section serves as a review of how accurately the PSA reflects the plant as characterized in the FSAR. In Section 2.1 the system success criteria for responding to the various transient events are covered. Section 2.2 is an evaluation of the support system requirements identified in the PSA for the various systems. In Section 2.3 assumptions regarding the configuration of the systems and human actions for both normal and emergency operations are discussed.

Section 3 contains the review of the application of PRA methods to the analysis. Section 3.1 is a discussion of the Initiating Event analysis, Section 3.2 contains the review of the event trees, and the system modeling is reviewed in Section 3.3. The quantification process is reviewed in Section 3.4, and the defining of plant damage states is discussed in Section 3.5. An overview of the dominant sequences is in Section 3.6.

Section 4.0 is a review of the PSA documentation, and Section 5.0 is a discussion of special topics and insights regarding the PSA. Conclusions are in Section 6.0.

Review comments in Sections 2 through 4 of this report are categorized into three areas:

A. Good Insights and Important Assumptions.

B. Items insufficiently explained.

C. Potential Problems to be Resolved.

1.1 Methodological Overview

The methodology used in the STP PSA is referred to as a "large event tree - small fault tree" technique. This methodology, developed by PLG Inc., emphasizes the development of very large accident sequence event trees with many detailed top events or split fractions in the PLG terminology. Each event tree top event is modeled by a single independent logic model such as a fault tree or block diagram. This process is significantly different than the methodology employed in NUREG-1150[4] and other NRC sponsored risk analyses. The NRC programs use what is described as a "small event tree - large fault tree" approach, where relatively simple event trees are developed to describe accident sequences, and extensive, highly dependent fault trees are developed to model the top events.

The PLG methodology does not model dependencies between systems and components explicitly in the top event or system models. Support systems and even operator actions are included as top events in the event trees along with front line systems. Each path through a particular event tree defines a unique sequence of events, and dependencies between events in the same sequence are handled by developing a model for each event which is dependent on any preceding event in the sequence. For example, if a particular sequence includes loss of electrical power as one top event and loss of Auxiliary Feedwater System (AFWS) a subsequent top event, then a fault tree for loss of AFWS given loss of electrical power is developed. This is in contrast to the typical NRC method where event trees define combinations of front line system failures. The NRC method models system dependencies by developing a fault tree for each front line system with support system fault trees linked or attached to the front line trees.

The two methods result in very different representations of final accident sequences which can render comparisons of results between studies very difficult. The NRC method propagates basic event faults from the system fault trees through the event trees to the sequence end states. It does this by first linking support system fault trees to front line fault trees, then merging the appropriate front line trees for each sequence, and then using Boolean reduction to arrive at a unique sequence expression with minimal cut sets of basic events. The PLG technique passes no basic event information from the system level models to the event trees, but rather each top event is quantified separately and the resulting value (or distribution for the uncertainty quantification) is propagated through the event tree model.

The result is that accident sequence models look very different between the two methodologies. PLG accident sequence models have no cut set or basic event representation, but are combinations of split fractions (top events) which have been modeled specifically to account for the relationships between the top events for each sequence. The NRC method yields sequence expressions in the form of Boolean equations with cut sets of basic events from the system fault trees.

Because of the fundamental differences between the methods, results must be compared carefully. A direct comparison between sequences from the two methods is not always possible. Comparisons must be made between similar types of accident sequences (e.g., station blackout). Importance measures cannot be directly compared between methodologies as well, because of the different techniques of propagating basic event failures through the accident sequence analysis.

Other differences exist, including common cause failure modeling, methods of sampling of uncertainty distributions, and failure rate values. However, much of the work PLG has done on common cause failures has been incorporated into the common cause analysis of NUREG-1150. In addition, many of the PLG basic event failure rates share common industry data with the NUREG-1150 data base. Differences between NUREG-1150 and the STP PSA regarding failure rates for similar components may arise. However, this last difference is more indicative of analyst choice or interpretation of data rather than fundamental methodological differences.

It should be noted that the purpose of this review is not to evaluate the validity of the PLG methodology for PRA. Both methods can produce correct results when applied properly. The purpose of this review is to evaluate the quality, thoroughness, and accuracy of the STP PSA analyses and to assess the legitimacy of the results.

1.2 Limitations of the Analysis

The STP PSA represents a detailed Level I risk analysis. The sophistication of the various models and analyses is generally consistent with state-of-the-art PRA practices. But as such, this analysis has limits of scope which are characteristic of PRA state of the art. Areas and issues not treated here include:

- Partial Failures
- Design Adequacy
- Adequacy of Test and Maintenance Practices
- Effect of Aging on component Reliability and Break in Phenomena
- Adequacy of Equipment Qualification
- Environmentally Related Common Cause
- Similar Parts Related Common Cause
- Sabotage

A further limitation of the STP PSA, which is consistent with current PRA practice, is the steam generator tube rupture initiator (SGTR). The STP PSA considered only single tube ruptures. Multiple tube rupture events have not been considered in even the most recent PRAs.

2.0 PLANT ASSUMPTIONS

This section of the report summarizes the review of the plant model to which PSA techniques were applied.

A great deal of effort was put forth in the PSA to understand plant systems. Section 5.4 of the PSA and the System Descriptions in the PSA provide excellent details of system operations, limitations, interfaces, and assumptions used to create risk models. The event sequence diagrams of Section 5.4 are well thought out and useful.

2.1 Success Criteria

Criteria of special importance are discussed in this section as they relate to system success.

2.1.1 Transients

A. Good Insights and Important Assumptions.

It is conservatively assumed that main feedwater is isolated following reactor trip. [Reference 1, Pages 5.4-10, 5.4-12, and 5.4-28]

It is conservatively assumed that steam dump utilizing the turbine bypass system is not available following reactor trip. [Reference 1, Page 5.4-28]

Criteria for Reactor Coolant Pump (RCP) seal cooling is provided, including the ability to utilize the positive displacement charging pump powered from the Technical Support Center (TSC) diesel generator given isolation of letdown. [Reference 1, Pages 5.4-13 and 5.4-35] Seal failure is assumed to result in a small LOCA which is equivalent to a hole 0.5 to 2 inches in diameter. [Reference 1, Pages 5.4-35, and Section 5.4.6, definition of small LOCA] Using the Moody Model as described in Reference 3, a two-inch hole discharges about 240 lbm/sec (water); Table B.3 of NUREG-1150, Reference 4, indicates that for a total of three RCPs using older design seal O rings, the leak rate can be substantially greater than 240 lbm/sec. The PSA addressed this concern by performing a sensitivity analysis on seal leak rate. Using a leak rate of 1900 gpm (approximately equal to the maximum RCP leak rate in NUREG-1150), the overall core melt frequency increased by only 2%. [Reference 1, Section 2.2.3]

The PSA did consider both pressure and temperature limitations on the use of RHR. [Reference 1, Page 5.4-17]

To maintain hot standby for an extended period of time, makeup water to the Auxiliary Feedwater Storage Tank (AFWST) must be provided. This requirement was factored into the PSA. [Reference 1, Page 5.4-27]

The PSA recognizes that an Engineered Safeguard Features Actuation Signal (ESFAS) isolates normal charging and letdown but does not isolate seal injection. [Reference 1, Pages 5.4-30 and 5.4-35]

A good discussion of how transients can progress to Loss of Coolant Accidents (LOCAs) was provided. [Reference 1, Pages 5.4-30 and 5.4-40]

The PSA accounts for the need to depressurize the primary system if a transition from hot standby to RHR cooling mode is desired. [Reference 1, Pages 5.4-18] Depressurization can be achieved by spray, control of makeup and letdown, or use of primary PORVs. It is implicit in the PSA, that during cooldown, pressurizer heaters are not required to maintain subcooling margin and allow use of RCPs. Ambient heat losses from the pressurizer and insurge of primary water to compensate for primary thermal contraction should not decrease pressure significantly when compared to the decrease in saturation pressure as primary temperature is reduced.

Should a transient event change to a small LOCA, High Head Safety Injection (HHSI) will be required. [Reference 1, Page 5.4-16] For sufficiently small LOCAs, eventual recirculation from the sump will require high head pumps given the inability to sufficiently depressurize the primary. The high head pumps pull directly from the sump during recirculation. Decay heat removal and containment cooling are provided by Reactor Containment Fan Coolers (RCFCs), not by the RHR heat exchangers. [Reference 1, Page 5.4-8 and 5.4-19] Containment cooling is discussed more fully in Section 2.1.8 of this report.

The discussion of transients in Section 5.4 of the PSA provides good insight into required operator actions. For example, following a normal trip with no transition to a LOCA, the operator must: control letdown and makeup, control main feedwater if available or auxiliary feedwater if actuated, control cooldown with turbine bypass steam dump or steam generator PORVs, control RCS pressure, borate as required, and initiate RHR if return to power is not an option.

B. Items Insufficiently Explained

Pressurized Thermal Shock (PTS) is of concern following a reactor trip if turbine trip fails and any Main Steam Isolation Valve (MSIV) fails to close. PTS is a possibility if the operator fails to manually throttle high head injection to maintain primary pressure within allowable limits as primary temperature decreases during the uncontrolled cooldown. [Reference 1, Pages 5.4-16 and 5.4-32] Numerical values for the failure of the operator to throttle high head injection and for the subsequent conditional probability of vessel failure from PTS could not be located in the PSA. [Reference 1, Table 5.4-5 does not provide a systems analysis reference section for Top Event VI, Reactor Vessel Remains Intact During PTS Challenge.

Successful end states following a transient are: hot standby, hot shutdown with Residual Heat Removal (RHR) cooling the plant toward cold shutdown, or return to power. There appears to be some confusion in nomenclature; numerous statements appear to refer to hot standby as hot shutdown [Reference 1, Pages 5.4-27, 5.4-29, 5.4-37.] In hot shutdown

RHR can be in operation; RHR cannot be in operation during hot standby if the definitions of Table 1.2 of Reference 5 are followed. The nomenclature in the PSA should be consistent with that in the Technical Specifications.

C. Potential Problems to be Resolved

Successful feed and bleed requires at least one train of High Head Safety Injection (HHSI) and manual opening of both pressurizer PORVs before steam generator dryout. [Reference 1, Pages 5.4-19 and 5.4-29.] High head charging pumps are not necessary for feed and bleed because the secondary water inventory in the steam generator provides for heat removal during the first 30 minutes of the transient after which decay heat is sufficiently low to allow depressurization with the PORVs and makeup with HHSI. Section B.1 of Reference 1 claims that over one hour is available before steam generator dryout. The time to dryout was discussed during the site visit in November 1989. A key parameter affecting time to dryout is how many full-power seconds occur between loss of feedwater and reactor trip. Reactor trip on low level will probably result in dryout in about 30 minutes, while if credit for earlier reactor trip on overtemperature delta T can be assured, dryout may not occur until after one hour. During the November meeting HL&P agreed to resolve this but has yet to do so.[6].

2.1.2 Large LOCAs

A. Good Insights and Important Assumptions

A large LOCA is a major breach in the primary system piping that rapidly depressurizes the primary system. As primary fluid flashes, both water and vapor blowdown through the break with incomplete phase separation and the vessel retains little water until Emergency Core Cooling System (ECCS) injection occurs. The PSA categorizes breaches greater than a six-inch diameter equivalent as a large LOCA. [Reference 1, Page 5.4-143.] This is a reasonable definition for a large LOCA, because at normal system pressure a six-inch hole discharges about 2200 lb/sec (water)[3], and the maximum ECCS injection rate from one train of HHSI and Low Head Safety Injection (LHSI) is 4000 gpm or 560 lb/sec with a completely depressurized primary [Reference 2, Figure 15.6-54.] Thus, a six-inch hole exhibits the characteristics of a major breach: rapid depressurization, emptying of the vessel, and the need for LHSI.

B. Items Insufficiently Explained

The PSA assumes that accumulator injection is not required following a large LOCA. [Reference 1, Pages 5.4-143.] This assumption needs to be justified. During the November 1989 site visit, HL&P agreed to address this item by either documenting the acceptable ECCS performance without accumulators or by adding a requirement for accumulator injection in the follow-on Level II PSA, but has yet to do so.[6]

The large LOCA event tree does not address the effect of failure to isolate containment on the ability to reflood the core. If the

containment pressure is lower than the minimum back pressure used in the LOCA licensing analyses, reflood occurs at a lower rate. [Reference 6, Sections 6.2.1.1.1.6 and 6.3.3, and Figure 6.2.1.5. Reference 7, Section 6.2.1.5.]

The PSA does not address long term switch over from cold to hot leg recirculation to avoid boron precipitation.

2.1.3 Medium LOCAs

A. Good Insights and Important Assumptions

A medium LOCA covers a range of breach sizes between a large and a small LOCA. At the upper end of the range, a medium LOCA is like a large LOCA. At the small end of the range, a medium LOCA is like a small LOCA where injection does not utilize LHSI.

The PSA categorization of breaches between two and six-inch equivalent diameter as medium LOCAs is reasonable. [Reference 1, Page 5.4-129.] LHSI would never be activated for a two-inch break since at 300 psia (LHSI shutoff) one HHSI train can inject 1200 gpm (168 lb/s) while the break flow would only be about 100 lb/s (water) using Moody's model. [Reference 2, Section 6.3 and Figure 15.6-54, Reference 3.] It is assumed in the PSA that no steam generator heat removal is required to remove decay heat, due to enthalpy losses out the break. This is a valid assumption. At 2500 psig (safety valves setpoint) a two-inch hole relieves 240 lb/s (water), and 1.7×10^5 Btu/s or 110 lb/s (steam) and 1.2×10^5 Btu. [Reference 3, Reference 8.] The change in enthalpy of 1.2×10^5 Btu/s can match decay heat at about 300 seconds after reactor trip [Reference 2, Figure 6.2.1.1-18.] During the first 300 seconds the excess decay heat would heat up the primary by about 15 degrees F at most, which would not saturate the primary.

B. Items Insufficiently Explained

The PSA assumes that accumulators are not needed to mitigate a medium LOCA. The resolution of this item is discussed in Section 2.1.2 along with large LOCAs.

2.1.4 Small LOCAs

A. Good Insight and Important Assumptions

A small LOCA requires HHSI for makeup and also requires steam generator cooling. Phase separation in the vessel occurs following a small LOCA if the RCPs are tripped. Breaches small enough to be handled by the normal Chemical and Volume Control System (CVCS) are categorized as transients. The PSA categorizes breaches between 0.5 and two-inch equivalent diameter as small LOCAs. [Reference 1, Page 5.4-109.] Based on Table 9.3-9 of Reference 2, the CVCS can match a leak of about 150 gpm (hot fluid) in excess of 100 gpm normal letdown since the maximum CVCS injection is 230 gpm charging plus 20 gpm seal injection. 150 gpm (hot fluid) is 14 lb/s. At normal primary pressure a 0.5 hole will discharge about 15 lb/s.(3)

Even if reactor trip on low pressure should occur no ESFAS actuation will occur since CVCS makeup can exceed loss through the hole above the ESFAS low pressure trip setpoint of 1850 psig.[5] Thus, 0.5 inches is an appropriate lower limit for small LOCAs. A two-inch upper limit for a small LOCA is acceptable. However, the details of primary to secondary cooling vary for different sizes of small LOCAs. For example, with steam generator cooling, the primary temperature will approximately equal the secondary temperature, about 550 degrees F. Saturation pressure at 550 degrees F is about 1000 psia. At 1000 psia one train of HHSI supplies about 700 gpm or 98 lb/s, but a break of size two inches relieves water in excess of this HHSI injection rate at 1000 psia. Thus, for certain small LOCAs the primary system will depressurize to saturation, flashing will occur, and condensation cooling of the primary side in the steam generators will be required.[9] However, one train of HHSI will, indeed, mitigate such a small LOCA.

In the recirculation mode, for breaches in the lower end of the small LOCA size range recirculation cooling will be with HHSI. The PSA claims that in this situation, RCFCs can remove decay heat and cool containment. [Reference 1, Page 5.4-121.] For high end small LOCAs, the primary system will depressurize to the point where LHSI can be used, which provides for heat removal through the RHR heat exchanger. Containment cooling is discussed in Section 2.1.8 of this report.

Given a small LOCA without Turbine Trip or MSIV closure, concerns related to PTS are handled as they were for a transient. [Reference 1, Pages 5.4-110 and 5.4-124.]

B. Items Insufficiently Explained

The PSA does not discuss breach of an instrument tube as a unique small LOCA. This breach is special because of its location being below the core. All other small LOCAs (which are in elevated piping) will uncover (steam out the break) prior to water level falling below the top of the core if the RCPs are tripped. However, the small size of the instrument tube (probably 5/8 inch) should ensure that HHSI can makeup the loss and retain subcooled natural circulation to the steam generators without break uncovery being necessary.[9] That is, the generic small LOCA success criteria probably covers instrument tube LOCAs. The PSA should address instrument tube LOCAs and ensure they are covered within the generic small LOCA category.

2.1.5 SGTR

A. Good Insights and Important Assumptions

The description of a Steam Generator Tube Rupture (SGTR) accident in Section 5.4 of the PSA is very thorough.

The PSA conservatively assumes core damage if the primary cannot be cooled to hot shutdown and RHR initiated. [Reference 1, Page 5.4-102.] It is possible to mitigate a SGTR by remaining in hot standby below the

steam generator PORV setpoint on the bad steam generator provided makeup to the AFWST is available.

The PSA conservatively assumes primary pressure must be controlled with spray, auxiliary spray or primary PORVs during cooldown. [Reference 1, Pages 5.4-106 and 5.4-107.] Plant Emergency Operating Procedures (EOP) do cover cooldown following a SGTR without pressurizer pressure control or with a saturated primary.[10,11]

2.1.6 V Sequence

A. Good Insights and Important Assumptions

The V sequence is an interfacing systems LOCA that bypasses containment. It should be noted that the RHR pumps and heat exchangers are inside containment at STP and thus their associated piping is not a potential initiator for the V sequence.

B. Items Insufficiently Explained

The PSA did not explicitly quantify the V sequence, claiming that since at least three valves in series must fail, the frequency of the sequence will be less than that that calculated for Seabrook.[12] The frequency of a large early release at Seabrook is small when consideration of mitigating actions is incorporated subsequent to the initiator. Without more discussion of the ability of the South Texas Plant to mitigate the initiating event, this comparison of the two plants is questionable even though the frequency of the initiating event is probably lower for the South Texas Plant than for the Seabrook plant. This concern should be addressed in the PSA. [Reference 1, Page 5.4-151 and table 5.4-30.]

Table 5.4-31 of the PSA is entitled "Piping Systems Connected to the RCS". This table fails to include the four-inch letdown line which penetrates containment. This line is not of concern for the V sequence due to the presence of flow orifices in the line inside containment which limit flow through a line break outside containment to within the CVCS makeup capability. [Reference 2, Section 15.6.2.2.] A break in the letdown line outside containment is thus categorized as a transient, not a LOCA. This point should be discussed in the PSA.

2.1.7 ATWS

A. Good Insights and Important Assumptions

The discussion in the PSA for the Anticipated Transient without Scram (ATWS) sequence is very thorough.

Vessel failure is assumed to not occur if ASME level C service conditions are maintained which correspond to an upper limit on primary pressure of 3200 psig. If 3200 psig primary pressure is exceeded, a small LOCA is postulated to occur. [Reference 1, Page 5.4-42.] The PSA requires boration given failure of rods to insert, to mitigate the ATWS.

[Reference 1, Page 5.4-41.] Boration is necessary to reduce power and lower pressure to allow for inventory makeup.

2.1.8 Containment Cooling

B. Items Insufficiently Explained

The PSA implies that spray injection and spray recirculation are not required for containment integrity, but are helpful for fission product removal. [Reference 1, Page 5.4-144.] Containment pressure will exceed the calculated pressures of Section 6.2, Reference 2, if there is no spray injection, but apparently it would not exceed the design value of 56.5 psig. However, the effect of no containment spray injection on containment pressure is not explicitly discussed.

Without spray recirculation, thermodynamic equilibrium between the sump water and the containment atmosphere is less closely achieved. This means the sump may be boiling which is acceptable because adequate NPSH for the ECCS pumps is available if the vapor pressure for the sump water is as low as the containment pressure due to vapor and air. [Reference 2, Section 6.3.2.2.] Spray recirculation removes no energy from containment at STP, but does help establish thermodynamic equilibrium.

Section 5.4 of the PSA states that during recirculation, either one RHR heat exchanger or two RCFCs can maintain containment integrity and match decay heat. [Reference 1, Pages 5.4-148, 5.4-149, 5.4-76.] These criteria are in conflict with those of Section 16 of the PSA which states both one RCFC and one recirculation heat removal path are required. [Reference 1, Page 16.1-5.] Also, Section 16 implies that recirculation always removes heat which is not true at STP when recirculating with HHSI pumps; only recirculation with LHSI pumps utilizes the RHR heat exchangers. The discrepancies between Sections 5.4 and 16 of the PSA should be resolved.

The PSA does not reference the basis for the adequacy of containment cooling with one LHSI loop in recirculation or two RCFCs. A rough calculation supports this criteria, but it is not justified in the PSA. The design maximum temperature of the ECCS pumps is 300 degrees F. [Reference 2, Table 6.3-1]. If it is assumed that the sump water reaches this temperature and that the containment sprays are not working, thermodynamic equilibrium between the sump and containment would not be established. The sump would be boiling and total containment pressure would be 68 psia, slightly below the containment design pressure of 71.2 psia. At 68 psia, air pressure is about 19 psia and hence vapor pressure is about 49 psia. Saturation pressure at 49 psia is 280 degrees F. With containment atmosphere at 280 degrees F, two RCFCs can remove about 220×10^6 Btu/hr from the containment; and with the sump water at 300 degrees F, one RHR heat exchanger (LHSI) can remove about 200 $X10^6$ Btu/hr from the sump water. [Reference 6, Figure 6.2.1.1.-3 and Table 6.2.11-5.] Decay heat would not reach 200×10^6 Btu/hr until approximately 4000 s after reactor trip. [Reference 2, Figure 6.2.1.1-18.] If recirculation is initiated at 1200 s (a reasonable time based on information in the FSAR) with the containment atmosphere at 235 degrees F, decay heat would

be about 280×10^6 Btu/hr [Reference 2, Table 6.2.1.1-10 and Figure 6.2.1.1-18.] The mismatch can be conservatively estimated as 80×10^6 Btu/hr into containment for 2800 s. Thus, a total of 62×10^6 Btu are added to containment before minimum containment cooling can match decay heat. This mismatch is acceptable because about 190×10^6 Btu would be required to generate saturated vapor in containment from 235 degrees F to 280 degrees F. Equipment operability under these minimum containment cooling conditions is not discussed in the PSA.

It is claimed in the PSA that a hole in containment greater than or equal to three inches in diameter will not allow containment to pressurize. [Reference 1, Page 5.4-73.] The basis for this claim is not clear. At a design pressure of 71.2 psia, a three-inch hole will relieve about 2.2×10^4 lb/hr of saturated vapor. [Based on equations in Reference 13.] If it is assumed that all decay heat generates steam and an enthalpy of phase change of 900 Btu/lb is used, this relief rate can match 1.98×10^7 Btu/hr of decay heat. However, this level of decay heat is not reached until about 10^6 seconds after reactor trip. [Reference 2, Figure 6.2.1.1-18.] The PSA does not justify the three-inch limit.

In accident scenarios in which recirculation from the sump is available, but with no containment heat removal via RHR heat exchanges or RCFCs, core melt is assumed to occur prior to containment failure. [Reference 1, Page 5.4-121, 5.4-135,5.4-146.] This is reasonable using 300 degrees F as the design limit for ECCS pumps since as previously discussed the 300 degrees F limit should be reached before the containment design pressure is reached. This point should be clarified in the PSA.

The PSA does not consider the possibility for early containment failure except for failure to isolate. [Reference 1, Section 5.4.4 and Table 16.1-6] Early containment failure is failure before or during core melt due to causes other than failure to isolate containment. It is stated in NUREG 1150 that early containment failure at large dry PWR containments is of low likelihood; however, direct containment heating following high pressure melt, or in-vessel steam explosion can cause early containment failure. These points should be mentioned in the Level I PSA but do not have to be substantiated until the Level II PSA is completed.

2.2 Support System Requirements

Tables 5.3-1 and 5.3-2 of the PSA summarize intersystem dependencies. The system descriptions appended to the PSA provide more details on support interfaces.

2.2.1 Electric Power

A. Good Insights and Important Assumptions

System dependencies on electric power for motive power appear to be completely identified. The 4160 Vac system includes the 480 Vac system. [Reference 1 system description 1 assumption 38.] Sources of electric power consist of: offsite power, the three 4160 Vac 1E trains including 480 Vac, the four DC 1E trains, and the four Vital 120 Vac trains.

The following requirements were correctly identified in the PSA:

- Pressurizer PORVs require DC to open.
- Pressurizer PORV block valves require 480 Vac to close.
- Steam Generator PORVs use hydraulic actuators and require 480 Vac. They also require 120 Vac and the Qualified Display Processing System (QDPS).
- Auxiliary Feedwater train D requires DC power to open isolation valves, no AC power is required for train D. Trains A, B, and C require 4160 Vac for pump motors and 480 Vac for isolation valve motors; DC power is required to close the circuit breakers to start the pumps. (4160 Vac motors are across-the-line starting and do not use motor starters.)
- MSIVs fail closed on loss of DC.
- Turbine bypass valves require DC to open.
- The CVCS centrifugal starting pumps require 4160 Vac for motors and DC for closing circuit breakers. The CVCS positive displacement pump motor requires 480 Vac. Valves require 480 Vac.
- The HHSI and the LHSI require 4160 Vac for pump motors and DC for circuit breakers. All motor operated valves (MOVs) are correctly aligned for injection but 480 Vac is required to operate valves when switching to recirculation.
- The Containment Spray System (CSS) requires 4160 Vac for pump motors, 480 Vac for valves, and DC for circuit breakers.
- The RCFCs require 480 Vac for fan motors and DC for circuit breakers.
- Containment isolation requires 480 Vac and DC.
- RHR, Component Cooling Water (CCW) and Essential Cooling Water (ECW) require 4160 Vac for pump motors, 480 Vac for valves, and DC for circuit breakers.
- Essential chilled water requires 480 Vac for pump motors. The PSA identifies a requirement for 1E DC also; however, this may not be necessary. These motors use motor starters in a motor control center and the AC power for closing contactors is derived from a stepdown transformer in the 480 Vac supply [wiring diagram 9ECH0701]. Only if circuit breakers upstream of the contactors are open is 1E DC required to close them.

2.2.2 Instrumentation and Control

The electrical requirements for Instrumentation and Control (I&C) were reviewed for both automatic control, and indication as required for manual control.

A. Good Insights and Important Assumptions

The following I&C dependencies for automatic actuation were correctly identified in the PSA:

- Automatic actions to trip the reactor and actuate safety equipment do not require control power. The Reactor Protection System (RPS) and the ESFAS both de-energize to trip except for the final bistable for initiating containment spray. [Reference 2, Section 7.3.1.2.2.1.]
- 1E DC is required for closing and tripping circuit breakers in 4160 Vac and 480 Vac circuits.
- 1E DC is required for diesel generator field flashing and emf control (The diesel generators do not use dedicated batteries, as verified in Reference 6.)
- 1E DC is required for the ESF Diesel Generator Load Sequencers.
- AC for 480 Vac motor starters in Motor Control Centers (MCC) is derived from the 480 Vac distribution to the MCC via a stepdown transformer.

The following I&C dependencies for reading instrumentation in conjunction with subsequent manual actions were correctly identified in the PSA (power for actuated components was discussed in the previous section):

- Solid State Protection System (SSPS) is necessary to reset ESFAS.
- SSPS requires 120 V vital ac.
- QDPS and associated inputs are needed to monitor plant conditions.
- QDPS requires 120 V vital ac.
- For control of Auxiliary Feedwater, QDPS and DC power are required for train D; QDPS and 120 Vac are required for trains A, B, and C.
- Switching ECCS from injection to recirculation mode requires SSPS for actuation on low RWST level.
- Essential chilled water needs QDPS for ECW valves on chillers.

- Other systems need I&C to provide information required for manual control; however, the ability to manually control these systems is not critical. Such systems include: CVCS, CCW, ECW, RHR heat exchangers/bypass, and boron addition.

B. Items Insufficiently Explained

For control of HHSI, QDPS is required. Without information on pressurizer level, throttling of HHSI as required (for example to avoid PTS) is not possible. This dependence is not identified in Table 5.3-2 of the PSA.

2.2.3 HVAC/Room Cooling

Room cooling is required to maintain equipment within design temperature limits. Heat sources within a room include: hot fluid, motors, and electrical switchgear. Heat removal is provided by building Heating Ventilating and Air Conditioning (HVAC) systems or by dedicated room coolers.

The requirements for safety grade cooling as discussed in section 9.4 of Reference 2 were compared to the dependencies indicated in Tables 5.3-1 and 5.3-2 of the PSA.

A. Good Insights and Important Assumptions

The following dependencies for HVAC/Room Cooling were correctly identified in the PSA:

- Control room HVAC Requires Essential Chilled Water to cool the chiller condensers in Air Handling Units (AHU).

- Essential Chilled Water requires ECW for a heat sink.

- Electrical switchgear requires the Electrical Auxiliary Building (EAB) HVAC.

- EAB HVAC requires Essential Chilled Water to cool AHUs. (Once through EAB HVAC is discussed in Section 2.3.2 of this report.)

- CCW pump rooms require supplementary coolers cooled by ECW. This is an additional dependence of CCW on ECW besides the need for CCW heat exchanger cooling. System Description 7 of the PSA for CCW indicates that ECW is necessary for both CCW heat exchanger cooling and for supplementary coolers.

- Diesel Generator rooms require once through ventilation using supply fans and intake/exhaust louvers. This dependence is not explicitly identified in Table 5.3-1; however, System Description 1 of the PSA for electrical power verifies that this dependence is considered as part of the standby power system itself.

- The ECW pump rooms require once through ventilation using supply fans and intake/exhaust louvers. This dependency is included as part of the ECW system itself. [Reference 1, System Description 4, Section J.9.].

B. Items Insufficiently Explained

The CVCS pump rooms require supplementary coolers cooled by CCW. This is an additional dependence of CVCS on CCW besides lube oil cooling for the centrifugal charging pumps. System Description 10 Section C of the PSA for CVCS indicates CCW is required for cooling all CVCS pump rooms. However, Section 1, assumption 9 of this system description states that analyses performed by HL&P indicates loss of room cooling for the positive displacement pump is acceptable. This analysis should be referenced, because an important finding of the PSA is that RCP seal injection can be provided by the PDP powered off the TSC diesel generator following station blackout.

C. Potential Problems to be Resolved

ECCS pump rooms require Essential Chilled Water according to Reference 2, Section 9.4. This dependence is not included in Table 5.3-2 of the PSA for LHSI, HHSI, and CSS. Table 5.3-2 does indicate that the ECCS pump rooms require EAB HVAC. Based on Reference 6, this entry is not necessary since it evidently accounts for an indirect dependence of the pump motors on the EAB HVAC. The EAB HVAC is necessary for cooling of the ECCS dependency on the 4160 Vac power supply switchgear for the ECCS pumps, but this dependence is already included as part of the ECCS dependency on the 4160 Vac system.

System Description 10 for safety injection, assumption J-2, states with respect to ECCS pump room cooling "...it is assumed that room cooling is not necessary due to natural convection that will be available."(1) This assumption is not justified. During the November, 1989 site visit, HL&P stated that they are investigating this issue.(5) During a tour of the plant in November, it was noted that the ECCS pump rooms are open to the Fuel Handling Building. Also, the RHR heat exchangers are inside containment, not in the ECCS pump rooms as they are at some plants. Thus, heat removal requirements for these rooms may be possible by natural circulation alone but this claim must be substantiated.

The utility supplied information on this issue in a letter dated January 16, 1990 from S. D. Phillips, Support Licensing.* In the letter, transient heatup analyses of the ECCS pump rooms were discussed. The analysis of most significance to the ECCS room cooling dependency issue is a study of the temperature profile of the pump rooms with no room cooling available, including the FHB HVAC system. The FHB and ECCS are linked by large passage ways which could allow for significant air flow between the two volumes. The analysis also assumed no natural convection between the pump rooms and the FHB. Thus, the analysis looked at heatup in "sealed" ECCS pump rooms.

*Letter to T. A. Wheeler from S. D. Phillips.

The analysis showed that an "enveloping temperature was reached in three days."[15] Unfortunately, the letter did not state what this enveloping temperature was. If this temperature was assumed to be 300 degrees F (maximum operating temperature of the ECCS pumps), then this analysis could be flawed. Electrical and control components which are located in the pump rooms may have a significantly lower maximum operating temperature. If the analysis correctly accounted for the maximum operational temperature of these components, then the three-day time period until this enveloping temperature is reached provided a very long recovery time window. Loss of ECCS pump room cooling is most probably not important in this circumstance. However, if the maximum operating temperature of the electrical and control components was not correctly incorporated into the analysis, then the issue of ECCS room cooling dependency has not been resolved.

2.2.4 Cooling Water

A. Good Insights and Important Assumptions

This section discusses the requirements for direct cooling of equipment; room cooling was discussed in the previous section.

The following requirements were verified to be correctly considered by the PSA:

- Emergency Diesel Generators are cooled by ECW
- CCW is cooled by ECW
- Essential Chilled Water is cooled by ECW
- RHR Heat Exchangers are cooled by CCW
- RCFCs are cooled by CCW
- CVCS centrifugal charging pumps lube oil is cooled by CCW
- RCP seals are cooled by either seal injection or CCW
- RCP motor is cooled by CCW
- RCP pump thermal barrier is cooled by CCW
- Auxiliary feedwater pumps are self cooled
- PDP pump in CVCS is self cooled [Systems Description 10, Section I, Reference 1.]
- HHI, LHI and CSS pumps are all self cooled. [Reference 2 and Reference 6.]

2.2.5 Instrument Air

A. Good Insights and Important Assumptions

Loss of Instrument Air (IA) is an initiating event because, among other things, it causes loss of main feedwater. The PSA does include loss of IA as an initiator. [Reference 1, Table 5.2.1.] This section reviews the impact of the loss of IA on mitigating systems. IA was not considered to be required for any mitigating system in the PSA; IA is not included in the system dependency Tables 5.3-1 and 5.3-2 of the PSA.

Section 9.3.1.3.1 of Reference 2 states that no safety components require accumulators to function properly. This design feature means that loss of IA is not of concern for safety related components at STP. (At other plants where accumulators are required, loss of IA should be considered because without recharging, accumulators may leak due to check valve failures.) IA is required for some non-safety components at STP. Air starting for DGs is provided by dedicated air compressors and storage receivers which are separate from the IA system. [Reference 2, Page 8.3-6 and page 8.3-24.]

Using Table 9.3-2 of Reference 2, the effect of loss of IA was examined for impact on the PSA. This review provided the following results:

- Main Steam System MSIVs Fail Closed (FC). This has no effect on the PSA since the PSA assumed main feedwater and turbine bypass are not available after reactor trip as discussed in Section 1.1.1 of this report.

- RHR heat exchanger valves Fail Open (FO) and heat exchanger bypass valves FC. This has no effect on the PSA.

- CCW radiation monitoring valves FC. This has no effect on the PSA.

- All air operated components in ECW, CVCS, control room HVAC, and EAB HVAC fail to safe position. This has no impact on the PSA.

- Diesel Generator ventilation dampers FO. This has no impact on the PSA.

- All air operated components in essential chilled water fail to safe position. This has no impact on the PSA.

- Cross connect valves in the AFW FC. This has no impact on the PSA since cross connection was not considered. [Reference 5]

- TBVs FC. This has no effect on the PSA due to no credit being given for steam dump after trip.

- Main feedwater flow control valves FC. Also, steam to pump turbines is lost since MSIVs FC. This has no effect on the PSA since no credit was given to main feedwater after trip.

- SG blowdown lines isolate. This has no impact on the PSA.
- ECW intake structure ventilation components fail to safe position. This has no impact on the PSA.

The assumption that IA is not required as an important mitigating system in the PSA appears to be correct.

B. Items Insufficiently Explained

Loss of IA has no effect on the PSA model as long as no credit is given for main feedwater or for turbine bypass steam dump after a trip. A more complete discussion of the justification for not concluding IA in the plant model would clarify this point.

2.3 System Lineups and Operations

This section highlights important aspects of the PSA related to standby system availabilities and off-normal lineups available to mitigate accidents.

2.3.1 Normal

A. Good Insights and Important Assumptions

At power, standby system known unavailabilities are limited by the technical specifications.[5] Major asymmetries in train unavailabilities as modeled in the PSA are summarized in this subsection.

For AFW, train D has a different unavailability than trains A, B, or C because D is turbine driven, DC controlled, and A, B, and C are motor driven, AC controlled. Technical specification 3.7.1.2 of Reference 5 places more stringent operability requirements on trains B and C than on train A. (This is probably because A and D share the same ESF actuation channel A.) The PSA indicates that the failure rate for train A is higher than the failure rate for Train B or C. In particular, failure rates for A and B (or C) are respectively: 8.6×10^{-2} (split fraction CDF) and 5.1×10^{-2} (CDH). [System Description 9, Reference 1]

For ECW, the PSA assumes train A is running, C is standby autostart, and B is off but available for manual start. [System Description 4, Assumption J.5, Reference 1] Thus the failure rate for B is highest, and the failure rate for C is higher than for A. In particular, failure rates for A, B, and C are, respectively: 9.4×10^{-4} (W11), 1.3×10^{-1} (W13), and 9.6×10^{-3} (W14).

For EAB HVAC, the PSA assumes Trains A and B are running and Train C is on standby. Thus failure of Train C is higher than A or B. [System Description 6, Assumption J.1, Reference 1.] In particular, failure rates for A (or B) and C are, respectively: 6.8×10^{-4} (F11), 4.5×10^{-2} (F13).

2.3.2 Emergency

A. Good Insights and Important Assumptions

Cross connection of AFW among steam generators was not considered as a possibility in the PSA.[8] This is a conservative assumption.

Feed and Bleed success criteria is based on Westinghouse calculations which justify the use of one HHSI train and both pressurizer PORVs. [Reference 1, Page 5.4-29] Credit for using only one PORV or vessel head vent is not given in the PSA.

RCP seal injection during station blackout is possible using the PDP charging pump powered by the TSC diesel generator. [Reference 1, Page 5.4-35]

ESFAS reset is required to throttle HHSI (to prevent PTS). [Reference 1, Page 5.4-14]

ECCS switchover from injection to recirculation is automatic.

Primary PORV motor operated block valves can be closed given failure of a PORV to reset. [Reference 1, Page 5.4-22] (Steam generator PORV block valves are manual valves, locked open.)

RCPs are tripped upon loss of CCW to bearing oil coolers to avoid vibration induced seal LOCAs. [Reference 1, Page 5.4-25]

AFW Storage Tank (AFWST) makeup is required to remain in hot standby. [Reference 1, Page 5.4-27]

Following an ATWS with inability to insert rods, boration is required. [Reference 1, Page 5.4-41]

On HHSI recirculation with no RCFCs, no containment heat removal is available. Operators can attempt to depressurize the primary with the steam generator PORVs to allow LHSI recirculation and heat removal by RHR heat exchangers. [Reference 1, Page 5.4-69]

Following a SGTR, operator action is required to isolate the bad generator and cooldown to hot shutdown where RHR can be used. [Reference 1, Section 5.4.5] The PSA conservatively does not take credit for the following scenarios given SGTR:

- Primary depressurization without PORVs, spray, or auxiliary spray. [Reference 1, Page 5.4-106]
- Remaining at hot standby below setpoint of PORV on bad steam generator with makeup to AFWST. [Reference 1, Page 5.4-102]
- Using turbine bypass steam dump as a way to depressurize secondary. [Reference 1, Page 5.4-102]

- Isolation of bad steam generator with other downstream valves if the MSIV fails to close given operator action. [Reference 1, Page 5.4-107]

B. Items Insufficiently Explained

If normal EAB HVAC is unavailable due to loss of cooling to AHU chiller condensers, the PSA assumes that once through (smoke purge) operation of EAB HVAC will prevent components from overheating. [Reference 1, System Description 6, Section B.6, E.6, J.3, and J.5] This is an important point; the PSA should reference the actual calculation justifying once through cooling with no AHU cooling.

The System Description for AFW states that decay heat removal with one steam generator is acceptable provided the PORV setpoint is reduced within 20 minutes after trip to lower the steam generator secondary temperature. [Reference 1, System Description 9, assumption J 2. and item B] The Plant Model implies that one steam generator fed with AFW can remove decay heat without its PORV being available. [Reference 1, Page 5.4-33] This difference in assumptions should be cleared up.

3.0 PROBABILISTIC SAFETY ANALYSIS FOR STP

This section of the report summarizes the review of the application of PSA techniques to the South Texas Plant.

3.1 Initiating Events

A. Good Insights and Important Assumptions

The PSA performed a comprehensive identification of initiating events. [Reference 1, Section 5.2] The following three methods were used to identify initiating events: Master Logic Diagram, Heat Balance Fault Tree, and Failure Modes and Effects Analysis. The final selection and grouping of initiating events is reasonable. [Reference 1, Section 5.2.4 and Tables 5.2-8]

The Failure Modes and Effects Analysis (FMEA) focused on plant specific support system failures of significance as initiating events. The FMEA was applied, to some degree, to all 212 STP systems and subsystems. The FMEA did not consider coincident, multiple failures among systems; however, such occurrences are sufficiently rare as to be eliminated from consideration. (The initiating phase of an accident can be defined as covering the time from the first event until reactor trip should occur, about ten seconds at most. The likelihood of subsequent failures occurring during this short interval is small. Failures following the initiating phase are modeled as mitigating system failures.)

B. Items Insufficiently Explained

Minor comments on the identification of initiating events are as follows:

- High and medium energy line breaks and cracks should be discussed more completely as potential initiating events. LOCAs, main steam line breaks, and feedwater line breaks are considered; however, the FMEA did not explicitly address other breaks such as one in the high energy steam line to the auxiliary feedwater train D drive turbine. Such events may be bounded by other events retained for detailed analysis as described in Section 5.2.4 of the PSA.

- The PSA does not justify excluding core blockage as an initiating event. Tables 5.2-6 and 5.2-7 indicates this event was identified but screened from further analysis.(1)

3.2 Event Trees

A. Good Insights and Important Assumptions

The PLG technique uses the large event tree, small fault tree approach. This technique develops models for a system which reflect the effect of prior system successes and failures. Event tree linking is used to correctly select the appropriate combination of system models for a given accident sequence. That is, the ordering of split fractions (top events)

in a particular sequence determines the appropriate system model to be used. A split fraction is the conditional probability of a system success or failure dependent on all previous system successes and failures.

The STP PSA contains four stages of event trees: two support and two frontline. The first stage event tree is for the electric power system, while the second stage event tree covers mechanical support systems. The third stage event tree models frontline systems through the early phase of an accident while the forth and final stage event tree models frontline systems during the latter phase of an accident. Section 4.3.5 of the PSA summarizes event tree linking which is a complex process. The procedure, as described, does indicate how a given split fraction is properly quantified; that is, the procedure addresses all prior failures and successes which form pre-existing conditions that affect the particular fault tree to be selected for each system in a given accident sequence. Both support system dependencies and the effect of the initiating event on the split fraction quantification are described.

The event trees are very complex due to the nature of the PLG technique. The PSA does an excellent job of describing the event tree development. The Event Sequence Diagrams (ESDs) which were developed as precursors to the frontline system event trees are extremely useful both as a development tool and as a road map for review. The PSA is careful to point out simplifying assumptions used in developing the event trees.

One preliminary concern about the event tree linking approach is how system dependencies are handled. That is, if a support system functions in a degraded manner, it may still impact quantification of another system. The PSA can account for such effects in either of two ways: an event tree may have more than two branches at a given event [Reference 1, Page 4.1-3], or special events can be added to the event tree.[6]

It is concluded that the STP event trees and the techniques utilized for event tree linking adequately account for accident sequence delineation and dependent effects.

3.3 System Modeling

A. Good Insights and Important Assumptions

The STP PSA does not provide graphic fault trees consisting of a road map of component failures combined in "and" and "or" gates. Due to the nature of the PLG techniques, the system component failures can be developed without such a graph. Support system failures are considered as boundary conditions on a system and are incorporated into sequence models by event tree linking as described in Section 3.2 of this report. Instead of graphic fault trees, block diagrams are utilized and Boolean equations for block failures are developed. [Reference 1, Section 4.2.2.1.1]

B. Items Insufficiently Explained.

The System Descriptions appended to the PSA adequately document system failure models at the component level; however, the documentation is not easy to review.

3.4 Quantification

This section provides a short summary of the PLG PSA techniques for quantifying internally-initiated core melt sequences and a discussion of the quantification aspects of the STP PSA.

3.4.1 Techniques

A. Good Insights and Important Assumptions

The quantification technique is discussed in sections 4 and Appendix A of the PSA.[1]

System level quantification is accomplished by convoluting Discrete Probability Distributions (DPD) for constituent components according to the failure or success logic created to model the system. Independent failures of identical components within a given system are correlated (DGs fail-to-start for example); there appears to be no correlation for identical components among different systems (MOVs fail-to-open for example). Common mode dependent failures are modeled using the Multiple Greek Letter (MGL) method. The DPD technique enables all types of probability distributions to be convoluted even if they are not well-behaved, lognormal in form.

The result of a system quantification is a probability distribution for a split fraction of an event tree. As summarized in Section 3.2 of this report, event tree linking is used to assemble the appropriate split fractions into an event sequence, and intersystem dependencies are accounted for by development of system failure models for each split fraction which as specified by the large event trees with appropriate boundary conditions for linking. The system quantification is rigorous in terms of consideration of probability distributions of constituent components; the resulting system probability distribution is a logical convolution of all component probability distributions rather than a point estimate quantification followed by an uncertainty model applied to important component failures.

Accident Sequences are quantified using point estimates (means) for each constituent split fraction. The PLG method tends to generate an unwieldy number of sequences, so the point estimate quantification is used to screen out nondominant sequences from further analysis. Important sequences are then subjected to a Monte Carlo uncertainty analysis and sequence probability distributions are produced. These probability distributions provide the final quantified results for the PSA.[4]

C. Potential Problems to be Resolved.

There appears to be no correlation for identical components in different systems. For example, similar events (e.g., MOVs fail to open) in two different system models (e.g., AFWS, ECCS) would not be correlated even if their quantification is based on the same entry in the data base.

3.4.2 Data Base

A. Good Insights and Important Assumptions

The PLG generic data base was the source of data for the STP PSA. [Reference 1, Section 7] This extensive data base provides probability distributions for numerous component-specific failures due to: hardware failures, common cause effects, and maintenance unavailability. No STP plant specific data was incorporated into the STP specific data base, because the data was developed prior to plant operation; however, the generic data was screened for applicability to STP components.

The data base is comprised of both nuclear power plant experience and industry data compilations. Component specific failure quantifications are provided in Section 7 of the PSA.

For some of the failure rates contributing to the more probable core damage sequences at STP, Table 3.4.2-1 compares the mean values used in the STP PSA with the generic ASEP mean values.(4)

Table 3.4.2-1
Sample Mean Failure Rates

Component Failure Mode	Mean of PLG Distribution	ASEP Value (Mean)
o Loss of off-site power	0.09/yr	0.11/yr*
o Diesel Generator, fail to start and run 24 hr (excluding test and maintenance)	0.10/demand	0.08/demand
o Turbine-Driven AFW Pump, fail to start and run 24 hr (excluding test and maintenance)	0.06/demand	0.04/demand

The PLG data base appears to be slightly more conservative than the ASEP data base; however, the difference is not substantial. Generally, the data base for the STP PSA is extensive and the quantification methods are state of the art.

Component specific data is provided in Section 7 of the PSA in tabular form; the mean, fifth percentile, median, and ninety fifth percentile

B. Items Insufficiently Explained

*Sequoyah specific analysis.(14)

points of the distribution for each specific failure are provided. These data tables do not provide units of the data, although the units can be deduced from the numerical values and from discussions accompanying the tables. In addition, there is no information on the specific distributions used to model the frequency distributions. It is not possible to reconstruct or understand the nature of the frequency distributions based on the limited information provided. For instance, Section 7 of the PSA contains several examples of deriving a distribution based on different types of data (e.g., generic data, operating experience). Some of the examples yield discrete distributions (see page 7.3-6 of Reference 1). Others yield continuous distributions which may be well defined, such as lognormal (Page 7.3-11), or numerically generated (Page 7.3-14). It is impossible to tell from the tables of the PSA data base which of these types of distribution is used for each frequency distribution.

3.4.3 Testing and Maintenance

A. Good Insights and Important Assumptions

Testing and Maintenance unavailabilities are discussed in Section 7.5 of the PSA.[1] Constituent causes include: repairs during operation, repairs following scheduled testing, scheduled testing, unscheduled repairs and testing, and preventative maintenance. Probability distributions on both the frequency and duration are used to develop unavailability probability distributions for a specific component.

The PLG generic data base served as the source of data. Plant specific features and site specific maintenance policies and procedures were used to correctly apply the generic data for frequency of maintenance to specific components. Plant specific technical specifications and component specific mechanical details were used to correctly apply the generic data for duration of maintenance to specific components.

The STP PSA considered asymmetries in train unavailabilities within a given system. This aspect was discussed in Section 2.3.1 of this report. Different maintenance-caused unavailabilities among trains within a given system can result due to the following reasons:

- A train may be operating, in auto standby, or in manual standby. (ECW for example.)
- One train may be comprised of different hardware than another. (AFW turbine driven, DC controlled train D for example, as contrasted with motor driven, AC controlled trains A, B, and C.)
- Technical specifications may allow different outage times among trains (AFW Train A can be inoperable longer than Trains B or C.)

The plant specific maintenance data for the STP PSA appears reasonable.

3.4.4 Common Cause

A. Good Insights and Important Assumptions

Common cause failures are modeled in the PLG generic data base through the Multiple Greek Letters (MGL) method. This method can be used to quantify common cause failures among more than two identical components. The PLG generic data base was used as the basis for common cause parameter quantification.[16] Data from this data base was screened for applicability to STP.

The consideration of common cause in the STP PSA appears complete. Section 7.4 of the PSA discusses common cause failures.[1]

3.4.5 Human Factors

A. Good Insights and Important Assumptions

The human error rates (HERs) used in the STP PSA were compared to values used for similar human errors by other PRA studies. The majority of the South Texas values were higher than those used by other studies, the remainder were within the same range of values. This somewhat tempers the concerns addressed in this section regarding the lack of documentation.

B. Items Insufficiently Explained

The comments presented in this section follow Section 15 of the STP PSA,[1] i.e., the comments on Section 15.1 and 15.2 are ordered such that they follow the presentation of the methodology in Sections 15.1 and 15.2.

The human actions analysis methodology is a combination of variations of three methodologies; SLIM, SHARP, and THERP.[17] How these methodologies are varied from their original derivation and why they have been changed is not documented. Also, as with many other HRA methodologies, SLIM has not been universally accepted by the HRA community.

<u>Section 15.1 and 15.2</u>

The goals listed for the human reliability analysis (see page 15.1-1, fourth paragraph) are important. One goal that has not been mentioned but is equally important, is the ability of an individual not involved in the original analysis to use the methodology presented to obtain duplicate Human Error Rate (HER) values. The methodology presented should enable the reader to reproduce the results.

The last paragraph of Section 15.1 states, "The methodology developed and used in evaluating the dynamic human actions in the event sequences and the recovery actions in this study is relatively new, it is believed to be a significant improvement over previous methodologies by providing a greater traceability to basic factors affecting human performance." What is the difference between the new methodology and that used previously

and what accounts for the "significant improvement"? In Section 15.2, the first paragraph attempts to describe the new methodology, "PLG has adopted an application of SLIM to quantify the event-level dynamic operator actions in the plant response model of a PRA." No reference has been given for SLIM. There are several versions of SLIM available, the majority of which are the SLIM-MAUD version. Therefore the version referenced in this review for comparison purposes is, The Use of Performance Shaping Factors And Quantified Expert Judgement in the Evaluation of Human Reliability: An Initial Appraisal, by David E. Embrey.[18] Documentation of the differences between David Embrey's SLIM version and that chosen for the STP PSA along with justification for the changes would help validate the methodology by emphasizing any improvements made.

There are some problems associated with the PRA application of SLIM. The following statements are excerpted from various sections of GRS Project RS688[19] which evaluated and compared various HRA methods. The following statements from Reference 19 highlight one HRA expert's opinion on why SLIM has limited use as an HRA procedure.

> SLIM uses individual judgements combined statistically, it requires structure and guidance for these judgments. Evidence on the consistency and validity of SLIM is unconvincing, more research is required. Direct outputs from SLIM are interval scale numbers called SLI numbers ranging from 0 to 100. The SLI numbers must be converted to estimated HEPs by means of calibration using HEPs from some objective source. Use of estimates obtained from some other psychological scaling technique should not be used to calibrate SLIM estimates. Calibration data can consist of in-plant HEPs or training simulator HEPs that are plant-specific. If simulator data are used as calibrators, analysts need to recognize the problem of the validity of the simulator data themselves. Calibrators are required for each homogeneous subset of tasks. The flexibility of SLIM enables it to treat any aspect of human behavior. Keep in mind that the direct outputs of SLIM are interval scale values, and must be calibrated if they are to be converted to HEPs to be used in a PRA. SLIM stresses the importance of specifying relevant Performance Shaping Factors (PSFs) so that all judges have the same PSFs in mind when making judgments. Judges consider one PSF at a time and do not appear to be instructed on how to handle any interactions. There is no method for handling discrepant group opinions in the consensus mode. Another objection to the methodology is the assumption that the likelihood of error in a particular situation depends on the combined effects of a small set of PSFs.

Section 15.2 of the PSA, page 15.2-1, states, "Seven PSFs have been selected to span the range of problems that operators face". A Performance Shaping Factor is any factor that influences human behavior. PSFs may be external to the operator or may be a part of his or her internal characteristics. As can be seen from its description, PSFs can be chosen from a wide variety of factors. The STP PSA does not document how their PSFs were narrowed down to seven or why these are the most

important. Following are some quotations on PSFs from the Embrey report[18]:

> ...a team of expert judges decides on a set of PSF which are deemed to be the major determinant of reliability in the broad category of tasks being considered.
>
> ...The composition of the panel of judges could include operators, supervisors, human factors specialists, and other experts with insight into the factors which could impact reliability. The derivation of the initial PSF set will involve direct interaction between subject matter experts in order to arrive at a consensus for the task categories concerned.
>
> ...If a group of judges is asked to derive a global set of PSF for a task category, it is possible that they may have differing mental models of the ways in which the PSF should be weighted or can combine, to produce the resulting probability of task success. The imposition of the simple reliability model on the experts judgement is a means of increasing the homogeneity of their perceptions of the situation, thereby assisting in reaching a consensus.

For the STP PSA, was a team of expert judges used to decide on the PSFs? Who were they and what are their credentials? Was a simple reliability model used?

The PSA describes an operator response form developed to document the factors affecting operator performance. Is Table 15.2-1, the scenario sheet form, the operator response form? If the scenario sheet form is the operator response form, it doesn't appear to provide a "qualitative assessment of the problems that the operator will face while undertaking an action" as described in the documentation. If these forms are not equivalent, where is the operator response form and what is the scenario sheet form?

The third paragraph of Section 15.2 states, "The quantitative evaluation of the HER is accomplished by assessment teams of operators and PRA team members...". Who were the people used as the expert judges? Did the mix of individuals used as judges provide varying sources of information? What training was provided to these experts? The following statements are some excerpts from the Embrey 1983 report[18] regarding expert judges:

> Multiple experts with varying sources of information are the most effective estimators of likelihoods as long as they are all reasonably knowledgeable regarding the area being considered.
>
> Training in probabilistic thinking can improve the judges' estimates. Training should also acquaint the judges with known biases which can affect judgements.

Is the weight of each PSF, w_i, the normalized weight? The derivation of the Success Likelihood Index (SLI) or Failure Likelihood Index (FLI) by

Embrey normalizes the weight for each PSF. After reading through the rest of the Section 15 documentation it does appear that the normalized weight is used.

The calibration tasks are selected from HERs determined by PRAs of other nuclear power plants. As stated previously, use of estimates obtained from some other psychological scaling technique should not be used to calibrate SLIM estimates.

The STP PSA adaptation of SLIM resulted in a series of steps. The first step refers to the methodology outlined in Steps 1 and 2 of SHARP. There is no reference given for SHARP. Therefore the assumed version used is EPRI NP-5546.[23] Step 1 also mentions a split fraction failure criteria but doesn't define the term.

Step 4 refers to the methodology outlined in Step 3 of SHARP and to Table 15.2-1 (the scenario sheet form). It is implied that use of the scenario sheet form implements the Step 3 SHARP methodology. But, the scenario form doesn't document the operating experience (e.g., plant-specific event write-ups, LERs and events from other plants) that were scrutinized for the tasks to identify mishaps and corrective actions taken. Nor does it document the influence parameters (e.g., method of detection, alarms available, coordination required). This is a large deviation from step 3 of SHARP. Was the intent to detail the task without including the influence parameters? A thermal hydraulic analysis is mentioned but no further information is given. A brief overview of what was done would be helpful.

Each of the seven PSFs have a descriptive scaling guide (see Table 15.2-2) that provides a method of achieving consistency when using several expert judges. The scaling guides look reasonable but there is no discussion of the methodology and individuals used to develop it.

Step 8 mentions a LOTUS 1-2-3 program that was developed to aid in the classification of operator actions in groups having similar PSF weights. No discussion of the methodology used for the program was provided.

None of the steps addressed what would happen if no consensus could be reached for the final rating of the group?

Section 15.3

The expected omission error rates and commission error rates (see Tables 15.3-1 and 15.3-2 respectively) are presented with no indication of where the rates originate or why these particular values are appropriate.

Justification is not given for the use of Figure 15.3-1 to determine the calibration error. The Seabrook PSA[12] was given as the source of the figure, but more specifics on its location in the document would be helpful.

A RISKMAN designator is mentioned on page 15.3-2 but no definition of this term has appeared in Section 15.

A future consideration for the human error designators used in Table 15.3-4 is to use designators that yield a description of the human error being modeled. This would eliminate the need to check back on the table for a memory refresher of what the human error designator represents. The description of Table 15.3-4 on page 15.3-2, "...and then the applicable situation from Table 15.3-3" leads to the column labeled, "Applicable Situation from Table 15-6", on page 15.3-6. Should these both indicate Table 15.3-2? It is not immediately obvious where the cumulative HER mean values on Table 15.3-4 originate. After some trial and error it was determined that they are an addition of the applicable situations from Tables 15.3-1 and 15.3-2. Better documentation would eliminate the trial and error process. The designator, ZHE01B, has two cumulative HER mean values associated with it, 6.1E-3 and 9.4E-3. Is this intentional? The human error rates listed on Table 15.3-4 were compared to the values used for similar human errors from the Grand Gulf and Peach Bottom NUREG-1150 analysis.[20,21] The majority of the South Texas values were higher, while the remainder were similar to those used in NUREG-1150.

Section 15.4

Section 15.4 begins with a description of what was done by the analysts from steps 4 through 11 in the methodology section (15.2). This brings up:

(1) What was done for step 1? What were some of the functions humans perform at each branch point in the preconstructed event tree? What classification system was chosen to ensure that significant human interactions are identified? What completeness checks were done?

(2) What was done for step 2? What screening technique was used to rank and select key interactions for detailed analysis? What were the results? What was the cut-off parameter? Were selected operator actions observed in the plant environment?

(3) What was done for step 3? The PSFs described in Section 15.2 are not presented as the final set of PSFs. But, Section 15.4 doesn't indicate anything else.

The comments on Section 15.1 and 15.2 on the scenario sheets, are applicable for this section also.

Section 15.4, page 15.4-1, third paragraph states, "...five full operating crews evaluated the dynamic human actions following a briefing on methodology." The PSA does not expand on this, and it is not possible to ascertain whether the briefing incorporated probabilistic training and debiasing as recommended by Embrey.[18]

The third paragraph of Section 15.4 mentions use of the letters H, M and L to provide input for the PSF weighting factor. But no discussion on what determines an H, M or L evaluation for PSFs is given. These evaluations don't appear to follow Embrey's SLIM methodology. Also, what was given to the eight evaluation teams (i.e., what documents, instruction) to aid them in their evaluations?

The HL&P training staff evaluation (Table 15.4-32) and the single shift supervisor evaluation (Table 15.4-33) contain all 43 actions. Some comment on this would be helpful.

The human action identifiers, HEOL02 and HEOL01, on Table 15.4-39 were labeled HEOL2 and HEOL1 on all of the other tables.

The fourth paragraph on page 15.4-1 of the PSA states,"Weighting factors of 10, 5, and 0 were assigned to PSF weights with letters H, M, and L, respectively. Then, these weighting factors were normalized to sum to one for each evaluated human action. Finally, these normalized PSF weights were averaged over all eight evaluations of the human actions." Use of this method yields an PSF weight averaged across all eight teams for each of the seven PSFs. The human actions are then grouped according to similar PSF weights over all seven PSFs. Three events were chosen to follow this methodology; HEOCH01, HEOB06 and HEOS02. (Our copy of the report is missing page 15.4-73, which restricts the number of PSFs available for review.)

Following the methodology description, the first step is to normalize the weighting factors to sum to one for each evaluation. Then average these over all eight evaluations. The PSFs checked were task complexity and stress, respectively. These are documented on Table 3.5.4-1.

Table 3.5.4-1 Task Complexity and Stress PSF Weights

Evaluation Teams	HEOCH01		HEOB06		HEOS02	
	Normalized PSF for:		Normalized PSF for:		Normalized PSF for:	
	Task Complexity	Stress	Task Complexity	Stress	Task Complexity	Stress
Team 1	5/45	5/45	5/45	5/45	5/45	5/45
Team 2	5/35	5/35	10/70	10/70	5/35	5/35
Team 3	5/35	0	5/55	10/55	10/55	0
Team 4	10/30	0	5/30	5/30	0	0
Team 5	0	0	0	10/35	10/20	0
Team 6	5/30	5/30	5/50	10/50	10/45	5/45
Team 7	0	0	10/40	0	0	0
Team 8	0	5/30	0	10/40	5/25	5/25
Average over all 8 evaluation teams:	.1121	.0734	.0764	.1985	.1698	.0706
STP results (from Table 15.4-39):	.12	.08	.09	.19	.17	.07

As can be seen, the values derived here do not exactly match the numbers from the STP PSA. Perhaps the methodology has been misinterpreted, but independent checks by several analysts came to the same conclusion.

Tables 15.4-34 through 15.4-38 are the five operating crew performance-shaping factor evaluation sheets. The documentation states, "Members of each operating crew worked together to develop one evaluation sheet/crew." How were disagreements handled?

More information is necessary on how the 30 dynamic human actions are classified into six groups, this is difficult to duplicate without a copy of the LOTUS 1-2-3 program used to do this task. A more detailed description than that provided or an example would help.

Use of SLIM requires that the SLI (or FLI) numbers be converted to estimated HEPs by means of calibration from some objective source (e.g., in-plant HEPs or training simulator HEPs that are plant-specific). As mentioned previously, the calibration task data source used by STP was other PRA studies. An impressive amount of effort went into the collection of the data. However, there is some concern with using data from other PRA studies as the calibration points. One study, the European Benchmark Exercise On Human Reliability Analysis,[22] reports:

> "...SLIM results were shown to be extremely (too?) dependent on data used as reference points for calibration. When no good reference data are available, application of SLIM is not indicated. The results of the test and maintenance case show that there is a good agreement between the estimates obtained by a same team (sic) using THERP and SLIM. However, it is our belief that the sensitivity of SLIM to the anchor point probabilities and the fact that those probabilities were, either explicitly or implicitly, taken from the THERP data base, create strong dependency between the SLIM and THERP results." The operational transient study case in states, "Considering the results within a same team (sic), the SLIM results always agree quite well with the results obtained by other methods, but this could be due to the calibration anchor points used. As already pointed out during the discussion of the test and maintenance results, this calibration has a large impact on the values obtained."

The calibration data chosen for each group of operator actions have PSFs associated with them, see Tables 15.4-47 through 15.4-52. How were these determined? It would appear that some judgement or interpretation is required by the analysts to get these.

The dynamic actions human error rates, Table 15.4-23, are reasonable. The values are consistent with those used in other PRA studies.

Section 15.2, the methodology, needs to tie into Section 15.4, the practice, more explicitly. It's not always clear how the two sections relate.

Section 15.5

Since the evaluation of the recovery actions follows the methodology presented in Section 15.2 (as does Section 15.4), the comments made on Section 15.4 apply for Section 15.5 as well.

The tables of recovery actions, Tables 15.5-19 and 15.5-20, for some recovery actions and some PIFs, have normalized the weighting factors. Is there any particular reason that some are normalized and some aren't? What is meant in the remarks column by the M:2.2-2, M:4.0-3, L:1.6-3, etc.?

The recovery actions human error rates, Table 15.5-37, look reasonable. The values are consistent with those used in other PRA studies.

Section 15.6

Overall the description of the methodology used for electric power recovery actions was good. There were a few items that were not clear which will be discussed in the following paragraphs.

There was no reference for the STADIC computer code. A better description of the code is required before an understanding of what the code does is possible.

QDG is a subroutine of what program? It is assumed the STADIC code but it's not stated in the document.

It's not clear how boundary conditions for a specific event scenario defines the power failure function or how the nature and timing of the failures determine the recovery distribution. An example would help clarify what was done.

The tables presented on pages 15.6-7, 15.6-8, 15.6-9 and 15.6-16 have values that can be associated with several other values. For example, the table on page 15.6-8 has a 0.5 value for time following operator response that corresponds to a probability of 0.20 and 0.10. Which value is used?

Justification for the probability values used on the table presented on page 15.6-9 would be helpful.

A MAPP analysis is mentioned on page 15.6-13 but no reference or information about it is provided.

3.5 Binning of Core Melt Sequences

A. Good Insights and Important Assumptions

To simplify the PSA, various pinch points are utilized. [Reference 1, Section 4.1.3.2.2.] A pinch point is a stage of the analysis for which the subsequent modeling is independent of how the stage was achieved. Every accident sequence that results in core melt can be categorized by

the timing of the melt, the thermodynamic state of the primary system at the point of melt, and the status of plant systems when the melt occurs. Thus, core melt is a pinch point in the analysis. Although a Level I PSA does not evaluate source terms, consideration of the state of containment is prudent to employ in the Level I PSA to adequately consider dependence among core coolin. and containment. Thus, the state of containment and its associated protection systems such as isolation, heat removal, and fission product scrubbing, are appropriate to include in the categorization of core melt accident sequences.

The STP PSA bins core melt sequences into four Plant Damage States (PDSs). [Reference 1, Figure 4.1-6, Figure 5.1-1 and Table 16.1-6.] The four PDSs are:

- PDS Group I: core melt with intact containment.
- PDS Group II: core melt with late containment failure.
- PDS Group III: core melt with small early release.
- PDS Group IV: core melt with large early release.

B. Items Insufficiently Explained

Although it is not required to rigorously justify the containment model in a Level I PRA, numerous aspects of the STP PSA containment model should be justified by the Level II PSA, or its equivalent. These aspects are discussed in Section 2.1.8, Containment Cooling, of this report and they are, in summary:

- The impact of no spray injection on containment integrity.
- The minimum complement of containment cooling components required for long term heat removal. Equipment operability under these conditions.
- The justification for three-inch equivalent diameter containment bypass as a criterion for containment pressurization.
- The assumption of core melt prior to containment failure given no heat removal.
- The possibility for early containment failure due to means other than failure to isolate.

3.6 Dominant Sequences

Section 2 of the STP PSA provides results of the Level I PSA. [Reference 1] The conclusion of the analysis is that the mean frequency of core melt is 1.7×10^{-4} per reactor per year, and is dominated by internal initiating events. The dominant sequence has a mean frequency of 1.2×10^{-5} and twenty other sequences have a mean frequency greater than 10^{-6}. These twenty one sequences constitute about 34% of the total core

melt frequency; the remaining 66% is due to many sequences, each of low frequency.

Table 2.1-3 of the PSA summarizes the top twenty one sequences. This table alone does not provide sufficient detail to evaluate the sequences in terms of constituent event tree split fractions. An additional table, "Analysis of Additional Top-Ranking Sequences to Mean Core Damage", was provided which enables each sequence to be examined in terms of contributing split fractions. This information is reproduced here as Table 3.6-1. With this additional table, it is possible to refer to the appropriate split fractions in the System Description notebooks of the PSA and identify dominant component-specific failures contributing to the sequence of interest. The remainder of this section is based on a detailed review of this table; reference to sequence number is consistent with this table in which the sequences are ordered in terms of decreasing frequency. Section 2.2 of the PSA summarizes the importance of various initiating events and mitigating system failures. The following conclusions were determined by review of Table 3.6-1 along with the System Descriptions. The conclusions agree with the results of Section 2.2 of the PSA.

A. Good Insights and Important Assumptions

The twenty one dominant sequences may be categorized by initiating event as follows:

- Eight are station blackout sequences initiated by loss of offsite power; Sequences 1, 2, 5, 6, 11, 12, 13, and 15.
- Five are initiated by loss of offsite power followed by loss of main feedwater; Sequences 10, 14, 17, 18, and 19.
- Two are initiated by normal reactor trip; Sequences 7 and 21.
- Two are initiated by a steam generator tube rupture; Sequences 16 and 20.
- Two are initiated by loss of EAB HVAC which leads to station blackout; Sequences 3 and 4.
- One is initiated by loss of main feedwater, Sequence 8.
- One is initiated by normal turbine trip, Sequence 9.

Station blackout is involved in ten of these twenty one sequences, eight of which are initiated by loss of offsite power and two of which are initiated by loss of cooling for electrical switchgear. Four of the twenty one sequences are initiated by anticipated transients; namely, reactor trip, turbine trip, and loss of main feedwater. Two of the twenty one sequences are cause by a steam generator tube rupture.

The importance of mitigating system failure, excluding recovery, in the twenty one dominant sequences can be summarized as follows:

- Failure of one, two, or three Diesel Generators (DG) occurs in twelve sequences. Failure of three DGs occurs in sequence 1 and 12. Failure of two DGs occurs in seven sequences; Sequences 2, 5, 10, 11, 14, 15, and 18. Failure of one DG occurs in three sequences; Sequences 6, 13, and 17.

- Failure of turbine driven AFW train D occurs in eleven sequences; Sequences 1, 2, 3, 10, 11, 13, 14, 17, 18, 19, and 21.

- Failure of required operator action occurs in five sequences; Sequences 7, 8, 9, 16, and 20.

- Loss of RCP seal cooling occurs in four sequences; Sequences 4, 5, 6, and 12.

- Failure of motor driven AFW trains occurs in six sequences; Sequences 10, 14, 17, 18, 19, and 21.

- Loss of ECW train B occurs in six sequences; Sequences 2, 6, 13, 15, 17, and 19.

- Loss of EAB HVAC train C occurs in four sequences; Sequences 5, 6, 11, and 13.

- Small LOCA due to a stuck open PORV contributes to one sequence; Sequence 15.

None of the twenty one dominant sequences are initiated by a LOCA. There are no dominant sequences involving LOCA initiators followed by loss of recirculation cooling (commonly labeled as AH, S_1H, and S_2H sequences from the NRC event tree method). Such sequences were dominant in some of the NUREG-1150 PWR studies. Dominant contributors to such sequences include failure to switch over from injection cooling to recirculation cooling, and loss of ECCS pump and room cooling. Since the STP ECCS pumps are self cooled, draw suction directly from the sump, and the PSA assumes no forced cooling is required for the ECCS pump rooms, failure of the ECCS systems to mitigate a LOCA is of low probability. As pointed out in Section 2.2.3 of this report the PSA does not fully justify the assumption that ECCS pump room cooling is not required. Transient induced LOCAs occur in five of the twenty one dominant sequences; Sequences 4,5,6,12 and 15. In each of these sequences, station blackout is involved and hence no ECCS is available due to lack of electrical motive power for injection pumps.

Station blackout by itself does not lead directly to an RCP seal failure. The PDP charging pump can be powered by the TSC diesel generator and seal failure occurs only if this capability is also lost. Four station blackout sequences involve loss of RCP seal cooling from the PDP; numbers 4,5,6, and 12. As discussed in Section 2.2.3 of this report, the PSA should reference the calculation supporting the assumption that PDP room cooling is not required.

The STP plant has one turbine driven AFW train, Train D. Of the ten dominant sequences involving station blackout, five involve loss of AFW train, D; numbers 1,2,3,11 and 13.

Loss of ECW train B contributes to six dominant sequences, while loss of Train A or B contributes to none of the twenty one dominant sequences. This is reasonable based on the assumption that ECW Train B is not as available as train A or C as discussed in Section 2.3.1 of this report.

Loss of EAB HVAC train C contributes to mitigating system failures in two of the dominant sequences, while loss of Train A or B contributes to mitigating system failures in none of the twenty one dominant sequences. This is reasonable based on the assumption that EAB HVAC train C is not as available as Train A or B as discussed in Section 2.3.1 of this report.

Both of the SGTR initiated dominant sequences involve operator failures to establish RHR cooling and hence negate the driving pressure for the loss of coolant out an unisolated, ruptured steam generator. Operator actions also contribute to mitigating system failures following three dominant sequences initiated by anticipated transients (reactor trip, turbine trip, and loss of main feedwater).

The System Descriptions included as part of the PSA can be used to identify specific mitigating system component related failures of significance to the twenty one dominant sequences. This can be done by identifying component failures contributing most to the split fractions within each dominant sequence. The following component-specific failures are important:

- Diesel generator failures are dominated by independent hardware failures of the required number of diesel generators to run for 24 hours, the mission time.
- AFW train D failures are dominated by failure of the turbine driven AFW pump to start and run for 24 hours.
- ECW train B failures are dominated by preventative maintenance.
- EAB HVAC train C failures are dominated by maintenance.
- Loss of PDP cooling to RCP seals is dominated by hardware and maintenance failures.

B. Items Insufficiently Explained

The table of the twenty-one dominant accident sequences, (Table 3.6-1 of this report) was not incorporated into the PSA itself. The tabular summary of dominant sequences in the PSA did not provide the information needed to determine exactly which split fractions constitute each dominant sequence.

C. Potential Problems to be Resolved

The table of dominant accident sequences appears to disagree with the System Description split fraction quantification[1] for sequences involving failure of motor driven auxiliary feedwater trains:

- For Sequences 10 and 17 in Table 3.6-1, the failure of AFW train D and train C is attributed to split fraction AFP, yet System Description 9 (AFW) identifies AFP as the failure of AFW Train D and Train A.

- For Sequence 14, the failure of AFW train D and Train B is attributed to split fraction AFP.

- For Sequence 18, the failure of AFW Train D (turbine driven) and Train A is attributed to split fraction AFQ; yet the System Description 9 identifies AFQ as the failure of two motor driven trains.

- For Sequence 19, the failure of AFW Train D and Train C is attached to split fraction AFO, yet the System Description 9 identifies AFO as the failure of two motor driven and one turbine driven AFW trains.

The System Description split fractions indicate that AFW train A failures are more likely than Train B or C failures as expected based on the discussion in Section 2.3.1 of this report. This trend is not consistent with Table 3.6-1.

Further confusion arises from conflicting descriptions of the same top event between Table 3.6-1 and Section 2.2 of the PSA. For example, in Sequence 1 of Table 3.6-1, top event (or split fraction) G3 is described as loss of "All Three Diesel Generators Supplying Safety Related 4160V Buses." In Table 2.2-2 of the PSA, it is also described as loss of all three DGs. However, in Table 2.2-3 of the PSA, G3 is described as "Failure of Diesel Generator 13 Given that Diesel Generators 11 and 12 Have Failed." Such inconsistencies make it very difficult to understand the sequence models.

4.0 DOCUMENTATION

This section summarizes the adequacy of the documentation provided in the PSA.[1]

4.1 Methodology

A. Good Insights and Important Assumption

The PLG methodology is adequately described in the STP PSA. A simple, complete example application of the methodology would assist in understanding the nuances of the techniques.

4.2 Plant Model

A. Good Insights and Important Assumptions

The documentation of the behavior of plant systems is well documented in the PSA.[1] The format of the System Descriptions is well suited to updating the PSA as plant modifications are performed.

The System Descriptions do not include simplified drawings. This is a disadvantage for the reviewer of the PSA; however, it does provide one important advantage for on-site application of the PSA. If analysts use controlled plant drawings (P&IDs, wiring diagrams, electrical one line and metering drawings, etc.) they are more likely to correctly evaluate the system-specific implications of complex design modifications.

The System Descriptions do not include fault tree graphs consisting of "and" and "or" gates. System block diagrams and Boolean equations adequately document the system model since the system model logic in the large event tree, small fault tree technique employed by PLG is not extremely complex.

4.3 PSA Applications and Results

A. Good Insights and Important Assumptions

Overall the documentation of the application of the PSA techniques to the plant model is quite good.

B. Items Insufficiently Explained

Documentation of the dominant sequences does not indicate which split fractions contribute to each sequence; Table 2.1-3 of the PSA does not provide this information. Table 3.2-1 of this report does identify sequence specific split fractions but it is not included in the PSA.

5.0 SPECIAL TOPICS

This section discusses the results of the STP PSA in the context of the plant design.

5.1 Discussion of Value for Overall Core Melt Frequency

The mean value for core melt at STP is 1.7×10^{-4} per reactor year and is dominated by internal initiating events. This value is larger than one might expect given that STP has three ECCS trains and four AFW trains. Mean core melt frequencies from internal initiators at other plants have been calculated as:[4]

- 4.1×10^{-5} for Surry
- 4.5×10^{-6} for Peach Bottom
- 5.7×10^{-5} for Sequoyah
- 4.0×10^{-6} for Grand Gulf
- 3.4×10^{-4} for Zion

Although direct comparisons of means are not valid for determining sweeping conclusions; they are useful for evaluating trends.

Five possible reasons for the higher mean frequency at STP are:

- PLG Raw Data Values as compared with other Data Base Values that have been used.
- Conservative quantification of DG failures.
- Only one turbine driven AFW train.
- The separation between the two units.
- Conservative quantification of Human Error.

The first four of these possibilities are discussed in this section; the sixth is discussed in Section 5.4 of this report.

As discussed in Section 3.4.2 of this report, the PLG data base appears to be slightly more conservative than other data bases; however, this difference should not have a major effect on overall results.

Twelve of the twenty one dominant sequences involve direct failure of one or more DGs following loss of offsite power. A fault exposure time of 24 hours was used for the DGs [Reference 1, System Description 1 item B.6]; however, in the event sequences, only one hour was allowed for recovery of offsite power [Reference 12]. Failure to run for 24 hours contributes substantially to DC failures. [Reference 1, Table 7.3-1 and System Description 1 Split Fractions G1, G2, G3.] A less conservative approach could change each of these sequences by about a factor of 0.5. Assuming 50% of overall core melt is due to such sequences, the mean frequency of core melt could be changed by a factor of about 0.75.

An additional conservatism is the LOSP recovery model. The STP PSA allowed only one hour to restore offsite power, yet the mission time of these sequences is 24 hours. Furthermore, the value for failing to restore offsite power within one hour is 0.47, versus NUREG-1150 values of 0.44 for Surry, 0.19 for Sequoyah, 0.19 for Grand Gulf, and 0.11 for Peach Bottom. The value used for the STP PSA may be accurate for the regional grid at STP, but the recovery model used to quantify LOSP sequences (only hour for recovery of any power related fault) causes the STP PSA results to be very dependent on the one-hour recovery event. NUREG-1150 LOSP recovery failures drop to 1E-2 after approximately 10 hours.

STP has only one turbine driven, DC controlled AFW train. An additional AC independent AFW train would lower those sequence frequencies where station blackout is followed by loss of all AFW. However, replacement of an existing AC dependent AFW train with another AC independent AFW train should not significantly lower the overall core melt frequency. Such a replacement would result in LOSP sequence models involving loss of all feedwater, with failure of two diesel generators and failure of two turbine driven AFW trains. LOSP sequences involving loss of all feedwater currently include failures of three DGs and failure of one turbine AFW train. The failure rates for a DG and for a turbine driven AFW pump are numerically close; split fraction G1 (one DG fails) is 0.12 and split fraction AFR (one AFW train fails) is 0.11. Thus, replacement of one motor driven AFW train with another turbine driven AFW train should not provide significant benefits.

The two units at STP are totally separated except for the common main reservoir and essential cooling pond. This separated design has advantages in that important support systems such as component cooling water and service water are not shared. However, the ability to manually cross tie between units could assist in recovery given an accident at one unit. The tradeoffs between enhanced recovery and the potential for additional, subtle failures arising from such a capability need to be evaluated before the effect of such a capability on core melt frequency can be evaluated. Cross tie capability has the potential for lowering core melt frequency.

5.2 Importance of Station Blackout

Of the twenty one dominant sequences, ten involve station blackout; eight are initiated by loss of offsite power and two are initiated by loss of EAB HVAC. Loss of EAB HVAC results in overheating of electrical switchgear which renders all 4160 Vac 480 Vac safety related power unavailable even without loss of offsite power. Following station blackout, core melt occurs due to loss of turbine driven AFW train D in five of these sequences, while core melt occurs due to loss of PDP RCP seal injection in four of these sequences. Core melt occurs due to failure of a pressurizer PORV to reclose in one of these sequences.

The STP PSA concludes that 53% of overall core damage is due to loss of offsite power as an initiating event. Of the twenty one dominant sequences, thirteen are initiated by loss of offsite power and of these

thirteen, eight lead to station blackout. Additional station blackout sequences arise from overheating of electrical switchgear due to loss of EAB HVAC. Thus, station blackout contributes substantially to the overall core melt frequency.

5.3 Contribution of LOCAs to Core Melt

LOCAs as initiating events contribute little to core melt. [Reference 1, Table 2.2-1] None of the twenty one dominant sequences are initiated by a LOCA. This is probably due to the fact that the ECCS pumps are self cooled and the PSA assumed that no forced cooling is required for the ECCS pump rooms. This lack of support system dependency for the ECCS pumps renders their failures relatively unlikely.

Transients leading to small LOCAs occur in five of the twenty one dominant sequences. In each of these five sequences, ECCS is unavailable due to station blackout. Four of the five sequences involve RCP seal failure due to loss of PDP supplied seal injection; one sequence involves a stuck open pressurizer PORV.

DRAFT

6.0 CONCLUSIONS

This section summarizes the conclusions of this review with respect to internal events.

In general, the STP PSA is a state-of-the-art risk assessment. The detail to which the plant was modeled and the engineering analyses justifying this model are usually good, although certain parts of the analyses are not sufficiently justified. Section 5.4 and the System Descriptions document the plant model. The data base method is well described. The PLG methodology is sufficiently described and its application to STP is covered; however, a simple example of the methodology would aid in understanding the nuances of the techniques. The dominant sequences are not adequately described in the PSA so that split fractions contributing to dominant sequences can be easily identified. The most significant concern regarding the PSA is a lack of documentation to support the Human Error Analysis.

A summary of those review comments previously specified in this report as potential problems to be resolved, is as follows:

- The time to steam generator dryout following loss of all feedwater is not fully justified. (Section 2.1.1 of this report)
- The ability of equipment in the ECCS pump rooms to operate without forced cooling to the rooms is not fully justified. (Section 2.2.3 of this report)
- The confusion regarding labeling split fractions AFP, AFQ, and AFO in the dominant sequences (Table 3.6-1) should be resolved. (Section 3.6 of this report)

A summary of those review comments previously specified as items insufficiently explained, is as follows:

- Quantification of the PTS split fraction is not clearly provided. (Section 2.1.1 of this report)
- The use of the nomenclature "hot standby" and "hot shutdown" are inconsistent with the definitions in the Technical Specifications. (Section 2.1.1 of this report)
- Accumulator injection following large or medium LOCAs is assumed to not be required. This assumption is not justified. (Sections 2.1.2 and 2.1.3 of this report)
- The effect of early failure to isolate containment on reflood, following a large LOCA, is not addressed. (Section 2.1.2 of this report)

- The need to switchover from cold to hot leg recirculation to avoid boron precipitation is not addressed. (Section 2.1.2 of this report)

- The instrument tube breach as a potentially unique small LOCA is not discussed. (Section 2.1.4 of this report)

- The ability of STP to mitigate a V sequence LOCA should be discussed to justify screening such sequences from the analysis. (Section 2.1.6 of this report)

- A discussion of the letdown line break is not provided. (Section 2.1.6 of this report)

- Minimum containment cooling requirements are not sufficiently discussed. (Section 2.1.8 of this report)

- The assumption of no early containment failure is not discussed. (Section 2.1.8 of this report)

- The three-inch criterion for containment pressurization in not justified. (Section 2.1.8 of this report)

- I&C necessary for throttling HHSI is not included. (Section 2.2.2 of this report)

- The ability of equipment in the PDP pump room to operate without forced cooling to the room is not justified. (Section 2.2.3 of this report)

- The exclusion of IA from the mitigating systems is not clearly justified. (Section 2.2.5 of this report)

- The ability of EAB HVAC to provide adequate cooling in a once through mode with no cooling provided to AHUs is not explicitly justified. (Section 2.3.2 of this report)

- The acceptability of one steam generator in removing decay heat without its PORV being available is not clarified in the System Description for AFW. (Section 2.3.2 of this report)

- The screening of high and medium energy line breaks and cracks as initiating events except for LOCAs, main steam line breaks, and feedwater line breaks is not justified. (Section 3.1 of this report)

- The justification for excluding core blockage as an initiating event is not provided. (Section 3.1 of this report)

- Units in the data base tables of Section 7 are not provided. (Section 3.4.2 of this report)

- The majority of the values used for the Human Error Rates (HERs) are conservative, the remainder are similar to values used in other PRA studies. The HER values used do not seem unreasonable but, how these values were derived is not always clear. (Section 3.4.5 of this report)

- The table of the twenty one dominant sequences which identifies split fractions contributing to each sequence, Table 3.6-1 is not included in the PSA. (Section 3.6 and Section 4.3 of this report)

- Quantification of LOSP sequences are such that the exposure time for the DGs and the time for recovery of offsite power are inconsistent. (Section 5.1 of this report)

DRAFT

REFERENCES

1. Pickard, Lowe, and Garrick, Inc., South Texas Project Probabilistic Safety Assessment, Houston Lighting and Power Company, PLG-0675, May, 1989.

2. Final Safety Analysis Report, South Texas Project Units 1 and 2, Docket Nos. 50-498 and 50-499, July, 1978 with amendments.

3. Lewis, E. E., Nuclear Power Reactor Safety, John Wiley and Sons, Inc., 1977, Figure 8-19.

4. Severe Accident Risk: An Assessment for Five US Nuclear Power Plants, NUREG-1150, June, 1989.

5. Houston Lighting and Power Company, Written Responses to Issues Related to STP PSA, received November 29, 1989.

6. Technical Specifications, South Texas Project Units Nos. 1 and 2, Docket Nos. 50-498 and 50-499, NUREG-1334, January, 1989.

7. Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, LWR Edition, NUREG-0800, June, 1987.

8. Keenan, J. H., and Keyes, F. G., Thermodynamic Properties of Steam, John Wiley and Suns, Inc., 1936.

9. Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Westinghouse-Designed Operating Plants, NUREG-0611, January, 1980, Figure VIII-1 and related discussion.

10. "SGTR with Loss of Reactor Coolant, Saturated Recovery Desired," STP Procedure EOP-1POP05-EO-EC32.

11. "SGTR without Pressurizer Pressure Control," STP Procedure EOP-1POP05-EO-EC33.

12. Pickard, Lowe, and Garrick, Inc. Seabrook Station Probabilistic Safety Assessment, Public Service of New Hampshire, PLG-0300, December 1983.

13. Flow of Fluids through Valves, Fittings, and Pipe, Crane Technical Paper No. 410, Twenty Third Printing, 1989.

14. Bertucio, R.C., et al., Analysis of Core Damage Frequency from Internal Events: Sequoyah, Unit 1, NUREG/CR-4550/ Vol. 5, SAND86-2084, February 1990.

15. Berry, et al., Review and Evaluation of the Zion Probabilistic Safety Study, NUREG/CR-3300, SAND83-1118, Volume 1, Sandia National Laboratories, Albuquerque, New Mexico, May 1984.

16. Mosleh A., et al., A Database for Probabilistic Risk Assessment of LWRs, Pickard, Lowe, and Garrick, Inc., PLG-0500, 1988.

17. Swain, A.D., and H.E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, August 1983.

18. Embrey, D. E. ,The Use of Performance Shaping Factors and Quantified Expert Judgment in the Evaluation of Human Reliability: An Initial Appraisal, NUREG/CR-2986, BNL-NUREG-51591, May 1983.

19. Swain, A. D., Comparative Evaluation of Methods for Human Reliability Analysis, GRS Project RS 688, Gesellschaft fur Reaktorsicherheit (GRS) mbH, Forschungsgelande, 8046 Garching, Federal Republic of Germany, July 1988.

20. Drouin, M. T., et al., Analysis of Core Damage Frequency: Grand Gulf, Unit 1 Internal Events, NUREG/CR-4550, SAND86-2084, Vol. 6, Rev. 1, Part 1, Sept. 1989.

21. Kolaczkowski, A. M., et al., Analysis of Core Damage Frequency: Peach Bottom, Unit 2 Internal Events, NUREG/CR-4550, SAND86-2084, Vol. 4, Rev. 1, Part 1, August 1989.

22. Poucet, A. ,The European Benchmark Exercise On Human Reliability Analysis, Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment PSA '89, American Nuclear Society, Inc., La Grange Park, Illinois, April 2-7, 1989 (pp. 103-110).

23. Spurgin, A.J., Benchmark of Systematic Human Action Reliability Procedure (SHARP), NP-5546, Electric Power Research Institute, Palo Alto, CA, December 1987.

Appendix 1: LIST OF ACRONYMS

AFW	Auxiliary FeedWater
AFWST	Auxiliary FeedWater Storage Tank
AHU	Air Handling Unit
AOV	Air-Operated Valve
ATWS	Anticipated Transient Without Scram
CCF	Common Cause Failure
CCW	Component Cooling Water
CDF	Core Damage Frequency
CET	Containment Event Tree
CIS	Containment Isolation System
CSS	Containment Spray System
CST	Condensate Storage Tank
CVCS	Chemical and Volume Control System
DCH	Direct Containment Heating
DG	Diesel Generator
DHR	Decay Heat Removal
DPD	Discrete Probability Distribution
EAB	Electric Auxiliary Building
ECCS	Emergency Core Cooling System
ECP	Essential Cooling Pond
ECW	Essential Cooling Water
EOP	Emergency Operating Procedure
ESD	Event Sequence Diagram
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature Actuation System
FC	Fail Closed
FHB	Fuel Handling Building
FMEA	Failure Modes and Effects Analysis
FO	Fail Open
FSAR	Final Safety Analysis Report
HBFT	Heat Balance Fault Tree
HEPA	High Efficiency Particle Air
HER	Human Error Rate
HHSI	High Head Safety Injection
HL&P	Houston Lighting & Power Company
HPI	High Pressure Injection
HVAC	Heat, Ventilating, and Air Conditioning
I&C	Instrumentation and Control
IPE	Individual Plant Examination
IVC	Isolation Valve Cubicle
LCO	Limiting Conditioning for Operation
LHSI	Low Head Safety Injection
LOCA	Loss of Coolant Accident
LOOP	Loss Of Offsite Power (preferred)

Appendix 1: LIST OF ACRONYMS (Continued)

LOP	Loss of Power
LOSP	Loss of Offsite Power
LWR	Light Water Reactor
MAB	Mechanical Auxiliary Building
MCC	Motor Control Center
MDP	Motor-Driven Pump
MFW	Main FeedWater
MGL	Multiple Greek Letters
MLD	Master Logic Diagram
MOV	Motor-Operated Valve
MSIV	Main Steam Isolation Valve
MSL	Mean Sea Level
NPSH	Net Positive Suction Head
NRC	U.S. Nuclear Regulatory Commission
O&M	Operation and Maintenance Manual
PDP	Positive Displacement Pump
PDS	Plant Damage State
P&ID	Piping and Instrumentation Diagram
PLG	Pickard, Lowe and Garrick, Inc.
PORV	Power-Operated Relief Valve
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
PTS	Pressurized Thermal Shock
PWR	Pressurized Water Reactor
QA	Quality Assurance
QDPS	Qualified Display Processing System
RCB	Reactor Containment Building
RCFC	Reactor Containment Fan Cooler
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RWST	Refueling Water Storage Tank
SBO	Station Blackout
SCS	Secondary Coolant System
SGTR	Steam Generator Tube Rupture
SIS	Safety Injection System
SRV	Safety Relief Valve
SSE	Safe Shutdown Earthquake
SSPS	Solid State Protection System
STP	South Texas Project
TBS	Turbine Bypass System
TBV	Turbine Bypass Valves
TDP	Turbine-Driven Pump

DRAFT

Table 3.6-1
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 1)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Offsite Power	9.0×10^{-2}	LOSP	Chapter 7.6 (See Note 1 Below)
System Failures Following Initiating Event	All Three Diesel Generators Supplying Safety Related 4160V Buses	4.5×10^{-3}	G3	Appendix F: Book 1
	Turbine Driven Auxiliary Feedwater Pump	1.1×10^{-1}	AFR	Appendix F: Book 9
Recovery Actions	Failure to Recover Auxiliary Feedwater Before Steam Generator Dryout (See Note 2 Below)	8.0×10^{-1}	RECV5	Chapter 5.6
	Failure to Recover Offsite Power Within One Hour	4.7×10^{-1}	ORL	Chapter 15.6
	Failure to Recover at Least One Failed Diesel Generator Within One Hour	8.4×10^{-1}	OMC	Chapter 15.6
	Total Sequence Frequency (See Note 3 Below)	1.2×10^{-5}		

Note 1: LOSP Initiating Event Frequency is given as 1.29×10^{-1} events per year in Table 7.6-1. Since this frequency is based on a calendar year, a 0.7 factor is applied to account for the time that the plant is at power. This applies to all sequences with the LOSP initiator.

Note 2: Combination of Equipment Failures Not Recoverable Before Steam Generator Dryout and Operator Errors During Auxiliary Feedwater Recovery. This also applies to all sequences with the RECV5 recovery factor.

Note 3: The Frequency for Successful Operation of the Remaining Systems is not shown, but is included in the Total Sequence Frequency. This applies to each sequence identified in this table.

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 2)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Offsite Power	9.0×10^{-2}	LOSP	Chapter 7.6
System Failures Following Initiating Event	Diesel Generators A and C,	1.9×10^{-2}	G2	Appendix F: Book 1
	Essential Cooling Train B (Hence Diesel Generator B)	1.3×10^{-1}	WBE	Appendix F: Book 4
	Turbine Driven Auxiliary Feedwater Pump	1.1×10^{-1}	AFR	Appendix F: Book 9
Recovery Actions	Failure to Recover Auxiliary Feedwater Before Steam Generator Dryout	8.0×10^{-1}	RECV5	Chapter 5.6
	Failure to Recover Offsite Power Within One Hour	4.7×10^{-1}	ORK	Chapter 15.6
	Failure to Recover at Least One Failed Diesel Generator With One Hour	8.4×10^{-1}	OMB	Chapter 15.6
	Total Sequence Frequency	5.6×10^{-6}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 3)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Electrical Auxiliary Building HVAC Cooling	6.0×10^{-3}	LOEAB	Chapter 7.6
System Failures Following Initiating Event	All Three Safety Related 4160V Buses (Direct Failure)	1.00	N/A	N/A
	Turbine Driven Auxiliary Feedwater Pump	1.1×10^{-1}	AFR	Appendix F: Book 9
Recovery Actions	Failure to Recover Turbine Driven Auxiliary Feedwater Pump Before Steam Generator Dryout	8.0×10^{-1}	RECV5	Chapter 5.6
	Total Sequence Frequency	4.5×10^{-6}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 4)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Electrical Auxiliary Building HVAC Cooling	6.0×10^{-5}	LOEAB	Chapter 7.6
System Failures Following Initiating Event	All Three Safety Related 4160V Buses (Direct Failure	1.0	N/A	N/A
	Positive Displacement Charging Pump (Seal LOCA - No Makeup)	9.3×10^{-2}	PDH	Appendix F: Book 10
Recovery Actions	None	N/A	N/A	N/A
	Total Sequence Frequency	4.3×10^{-6}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 5)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Offsite Power	9.0×10^{-2}	LOSP	Chapter 7.6
System Failures Following Initiating Event	Diesel Generators A and B,	1.9×10^{-2}	G2	Appendix F: Book 1
	Electrical Auxiliary Building HVAC Fan Train C	4.5×10^{-2}	FCM	Appendix F: Book 6
	Technical Support Center Diesel Generator and Positive Displacement Charging Pump	2.0×10^{-1}	PDJ	Appendix F: Book 10
Recovery Actions	Failure to Recover Offsite Power Before Switchgear Overheats	4.7×10^{-1}	ORK	Chapter 15.6
	Failure to Recover at Least One Failed Diesel Generator Before Switchgear Overheats	8.4×10^{-1}	OMB	Chapter 15.6
	Total Sequence Frequency	3.6×10^{-6}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 6)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Offsite Power	9.0×10^{-2}	LOSP	Chapter 7.6
System Failures Following Initiating Event	Diesel Generator A;	1.2×10^{-1}	GAA	Appendix F: Book 1
	Essential Cooling Train B (Diesel Generator B); and	1.3×10^{-1}	WBE	Appendix F: Book 4
	Electrical Auxiliary Building HVAC Train C	4.5×10^{-2}	FCM	Appendix F: Book 6
	Technical Support Center Diesel Generator and Positive Displacement Charging Pump	2.0×10^{-1}	PDJ	Appendix F: Book 10
Recovery Actions	Failure to Recover Offsite Power Before Switchgear Overheats	4.7×10^{-1}	ORJ	Chapter 15.6
	Failure to Recover at Least One Switchgear Failed Diesel Generator Before Overheats	8.4×10^{-1}	OMA	Chapter 15.6
	Total Sequence Frequency	2.6×10^{-6}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 7)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Reactor Trip	$1.4 \times 10^{+0}$	RT	Chapter 7.6
System Failures Following Initiating Event	No System Failures - Failure of Long-Term Operator Actions to Stabilize the Plant	2.7×10^{-6}	ONA	Chapter 15.4
Recovery Actions	None	N/A	N/A	N/A
	Total Sequence Frequency	2.6×10^{-6}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 8)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Partial Loss of Main Feedwater Flow	$1.1 \times 10^{+0}$	PLMFW	Chapter 7.6
System Failures Following Initiating Event	No System Failures - Failure of Long-Term Operator Actions to Stabilize the Plant	2.7×10^{-6}	ONA	Chapter 15.4
Recovery Actions	None	N/A	N/A	N/A
	Total Sequence Frequency	2.2×10^{-6}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 9)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Turbine Trip	$1.1 \times 10^{+0}$	TT	Chapter 7.6
System Failures Following Initiating Event	No System Failures - Failures of Long-Term Operator Actions to Stabilize the Plant	2.7×10^{-6}	ONA	Chapter 15.4
Recovery Actions	None	N/A	N/A	N/A
	Total Sequence Frequency	2.0×10^{-6}		

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 10)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Offsite Power	9.0×10^{-2}	LOSP	Chapter 7.6
System Failures Following Initiating Event	Diesel Generators A and B	1.9×10^{-2}	G2	Appendix F: Book 1
	Turbine Driven and Motor Driven Train C Auxiliary Feedwater Pumps	4.9×10^{-3}	AFP	Appendix F: Book 9
	Closed Loop RHR Cooling Disabled	1.0	N/A	N/A
Recovery Actions	Failure to Recover Offsite Power Within One hour	4.7×10^{-1}	ORK	Chapter 15.6
	Failure to Recover at least One Failed Diesel Generator Within One Hour	3.4×10^{-1}	OMB	Chapter 15.6
	Total Sequence Frequency	2.0×10^{-6}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 11)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Offsite Power	9.0×10^{-2}	LOSP	Chapter 7.6
System Failures Following Initiating Event	Diesel Generators A and B,	1.9×10^{-2}	G2	Appendix F: Book 1
	Electrical Auxiliary Building HVAC Train C	4.5×10^{-2}	FCM	Appendix F: Book 6
	Turbine Driven Auxiliary Feedwater Train	1.1×10^{-1}	AFR	Appendix F: Book 9
Recovery Actions	Failure to Recover Offsite Power Before Switchgear Overheats	4.7×10^{-1}	ORK	Chapter 15.6
	Failure to Recover at Least One Failed Diesel Generator Before Switchgear Overheats	8.4×10^{-1}	OMB	Chapter 15.6
	Failure to Recover Auxiliary Feedwater Before Steam Generator Dryout	8.0×10^{-1}	RECV5	Chapter 5.6
	Total Sequence Frequency	1.9×10^{-6}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 12)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Offsite Power	9.0×10^{-2}	LOSP	Chapter 7.6
System Failures Following Initiating Event	All Three Diesel Generators Supplying Safety Related 4160V Buses	4.5×10^{-3}	G3	Appendix F: Book 1
	Technical Support Center Diesel Generator and Positive Displacement Charging Pump	2.0×10^{-1}	PDJ	Appendix F: Book 10
Recovery Actions	Failure to Recover Offsite Power Within One Hour	4.7×10^{-1}	ORL	Chapter 15.6
	Failure to Recover at Least One Failed Diesel Generator Within One Hour	8.4×10^{-1}	OMC	Chapter 15.6
	Failure to Recover at Least One Failed Diesel Generator or Offsite Power Before RCP Seal LOCA Uncovers Core (Conditional on Failure to Recover Power Within One Hour)	7.7×10^{-2}	RECV2	Chapter 5.6
	Total Sequence Frequency	1.8×10^{-6}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 13)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Offsite Power	9.0×10^{-2}	LOSP	Chapter 7.6
System Failures Following Initiating Event	Diesel Generator A;	1.2×10^{-1}	GAA	Appendix F: Book 1
	Essential Cooling Train B (Diesel Generator B); and	1.3×10^{-1}	WBE	Appendix F: Book 4
	Electrical Auxiliary Building HVAC Train C	4.5×10^{-2}	FCM	Appendix F: Book 6
	Turbine Driven Auxiliary Feedwater Train	1.1×10^{-1}	AFR	Appendix F: Book 9
Recovery Actions	Failure to Recover Offsite Power Before Switchgear Overheats	4.7×10^{-1}	ORJ	Chapter 15.6
	Failure to Recover at Least One Failed Diesel Generator Before Switchgear Overheats	8.4×10^{-1}	OMA	Chapter 15.6
	Total Sequence Frequency	1.7×10^{-6}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 14)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Offsite Power	9.0×10^{-2}	LOSP	Chapter 7.6
System Failures Following Initiating Event	Diesel Generators A and C	1.9×10^{-2}	G2	Appendix F: Book 1
	Turbine Driven and Motor Driven Train B Auxiliary Feedwater Pumps	4.9×10^{-3}	AFP	Appendix F: Book 9
	Closed Loop RHR Cooling Disabled	1.0	N/A	N/A
Recovery Actions	Failure to Recover Offsite Power Within One Hour	4.7×10^{-1}	ORK	Chapter 15.6
	Failure to Recover at Least One Failed Diesel Generator Within One Hour	8.4×10^{-1}	OMB	Chapter 15.6
	Total Sequence Frequency	2.0×10^{-6}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 15)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Init[illegible]ent	Loss of Offsite Power	9.0×10^{-2}	LOSP	Chapter 7.6
Sys[illegible]res	Diesel Generators A and C,	1.9×10^{-2}	G2	Appendix F: Book 1
Fol[illegible] Init[illegible]ent	Essential Cooling Train B (Hence Diesel Generator B)	1.3×10^{-1}	WBE	Appendix F: Book 4
	Pressurizer PORV Stuck Open	5.0×10^{-2}	PRA	Appendix F: Book 11
Recovery Actions	Failure to Recover Offsite Power Within One Hour	4.7×10^{-1}	ORK	Chapter 15.6
	Failure to Recover at Least One Failed Diesel Generator Within One Hour	8.4×10^{-1}	OMB	Chapter 15.6
	Failure to Recover Offsite Power or at Least One of the failed Diesel Generators Before the Core Uncovers due to the Stuck Open PORV (Conditional on Failure to Recover Power Within One Hour)	4.9×10^{-1}	RECV8	Chapter 5.6 (See Note 4 Below)
	Total Sequence Frequency	1.5×10^{-6}		

Note 4: During HL&P's Review, it was discovered that RECV7 is appropriate when two Diesel Generators Have Failed. RECV7 is 5.2×10^{-1}. As a result, the Sequence Total Frequency should be 1.6×10^{-6}.

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 16)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Steam Generator Tube Rupture	2.8×10^{-2}	SGTR	Chapter 7.6
System Failures Following Initiating Event	Failure to Depressurize Reactor Coolant System Below Steam Generator PORV Setpoint	3.1×10^{-3}	ODA	Chapter 15.4
Recovery Actions	Failure to Cool Down and Align Plant for Closed Loop RHR Cooling	2.9×10^{-2}	OAA	Chapter 15.5
	Total Sequence Frequency	1.4×10^{-6}		

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 17)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Offsite Power	9.0×10^{-2}	LOSP	Chapter 7.6
System Failures Following Initiating Event	Diesel Generator A;	1.2×10^{-1}	GAA	Appendix F: Book 1
	Essential Cooling Water Train B (Hence Diesel Generator B)	1.3×10^{-1}	WBE	Appendix F: Book 4
	Turbine Driven Train D and Motor Driven Train C Auxiliary Feedwater Pumps	4.9×10^{-3}	AFP	Appendix F: Book 9
	Closed Loop RHR Cooling Disabled	1.0	N/A	N/A
Recovery Actions	Failure to Recover Offsite Power Within One Hour	4.7×10^{-1}	ORJ	Chapter 15.6
	Failure to Recover at Least One Failed Diesel Generator Within One Hour	8.4×10^{-1}	OMA	Chapter 15.6
	Total Sequence Frequency	1.4×10^{-6}		

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 18)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Offsite Power	9.0×10^{-2}	LOSP	Chapter 7.6
System Failures Following Initiating Event	Diesel Generators B and C	1.9×10^{-2}	G2	Appendix F: Book 1
	Turbine Driven Train D and Motor Driven Train A Auxiliary Feedwater Pumps	1.9×10^{-2}	AFQ	Appendix F: Book 9
	Closed Loop RHR Cooling Disabled	1.0	N/A	N/A
Recovery Actions	Failure to Recover Offsite Power Within One Hour	4.7×10^{-1}	ORK	Chapter 15.6
	Failure to Recover at Least One Failed Diesel Generator Within One Hour	8.4×10^{-1}	OHB	Chapter 15.6
	Total Sequence Frequency	1.4×10^{-5}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 19)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Loss of Offsite Power	9.0×10^{-2}	LOSP	Chapter 7.6
System Failures Following Initiating Event	Essential Cooling Water Train B (Hence Diesel Generator Train B)	1.3×10^{-1}	WBC	Appendix F: Book 1
	Turbine Driven Auxiliary Feedwater Pump D and Motor Driven Pump C	3.8×10^{-4}	AFO	Appendix F: Book 9
Recovery Actions	Failure to Recover Offsite Power Within One Hour	4.7×10^{-1}	ORI	Chapter 15.6
	Total Sequence Frequency	1.1×10^{-6}		

DRAFT

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 20)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Steam Generator Tube Rupture	2.8×10^{-2}	SGTR	Chapter 7.6
System Failures	None	N/A	N/A	N/A
Recovery Actions	Failure to Isolate Stuck Open PORV or Safety Valve on Affected Steam Generator	2.4×10^{-2}	SLA	Appendix F: Book 8
	Failure to Align Plant for Closed Loop Cooling	2.6×10^{-3}	OCA	Appendix F: Book 17
	Total Sequence Frequency	1.1×10^{-6}		

Table 3.6-1 (Cont.)
Additional Analysis of Top-Ranking Sequences for Mean Core Damage Frequency
(Sequence 21)

Sequence Element	Event Description	Mean Frequency (per year)	Split Fraction Identifier	Reference (PSA)
Initiating Event	Reactor Trip	$1.4 \times 10^{+0}$	RT	Chapter 7.6
System Failures Following Initiating Event	All Four Auxiliary Feedwater Trains	3.4×10^{-5} 7.8×10^{-1}	CDA AFA	Appendix F: Book 9
Recovery Actions	Failure to Start Bleed and Feed Cooling Through Both Pressurizer PORVs	4.8×10^{-2}	OBA	Chapter 15.4
	Failure to Recover Auxiliary Feedwater Flow Before the Steam Generators Dryout	1.0	N/A	N/A
	Total Sequence Frequency	1.1×10^{-6}		