19R Probabilistic Flooding Analysis

The information in this section of the reference ABWR DCD, including all subsections, tables, and figures, is incorporated by reference with the following departures and supplements.

STP DEP T1 5.0-1 (Figure 19R-6)

STP DEP 10.4-2

19R.4.2.4 Watertight Doors

STP DEP T1 5.0-1

ECCS equipment rooms on the first floor of the reactor and control buildings have watertight doors. Also, external entrances to the control and reactor buildings below flood *level* (Refer to Section 3.4) *have watertight doors. The entrance to other divisional rooms have fire rated doors. These doors are normally closed and are included in the security surveillance system. These doors can be opened only with a card key and if left open security personnel will be alerted immediately. This system gives high assurance that the divisional separation will not be breached due to a door being inadvertently left open. The alarm system can detect if a watertight door is closed but not if it is dogged. A once per shift walkdown will ensure that watertight doors remain dogged when not in use.*

19R.4.3 Turbine Building Features

STP DEP 10.4-2

If either the circulating or turbine service water systems were to develop a leak and flood the turbine building, several features exist to mitigate the consequences of the flood. There are four circulating water pumps and three turbine service water pumps with *three circulating water pumps and two turbine service water pumps* in operation *supplying water* from the intake structure to the screenhouse *to the turbine building. Each pump has an associated motor operated isolation valve* with the isolation valve on the standby circulating water pump closed. *The condenser pit has redundant water level sensors arranged in a two-out-of-four logic. If flooding were to occur, the level sensors would alert the control room operator, trip the CWS pumps and close CWS valves. For breaks in the TSW system, adequate time (greater than 2 hours) is available for operator action to trip pumps, or close isolation valves, or open the truck entrance door.*

19R.5.3 Turbine Building

STP DEP 10.4-2

The following site-specific supplement addresses the STP Site being a high PCHS design and having all openings to safety-related buildings below flood level closed.

The circulating water system (CWS) has ~~three~~ four *pumps* located in the main intake structure *and each pump has an associated motor operated isolation (shutoff) valve.* Three of the pumps are normally operating and the fourth pump will be in standby with its associated isolation valve closed. *The turbine service water (TSW) system has three pumps and three motor operated isolation valves. For ~~a~~* the *high power cycle heat sink plant design* at STP 3 & 4 *(i.e., the heat sink is at an elevation higher than grade level of the turbine building), an additional isolation valve is installed in each line. All of these are classified as non-safety grade equipment. If a large pipe break develops either in the CWS or TSW piping and initiates flooding in the turbine building, it is necessary ~~either to trip all of the pumps (for a low heat sink) or~~ to close all of the valves of the associated system to terminate the flood. Four redundant safety grade water level sensors (operating in a two-out-of-four logic) in the condenser pit of the turbine building will generate a signal to alert the control room operator and trip all pumps and close all isolation valves in the CWS. TSW breaks must be manually mitigated but, due to the lower flow rate (Compared to CWS), sufficient time is available to trip the pumps or close isolation valves from the control room. A turbine trip and reactor shutdown will be initiated as a consequence of turbine building flooding.*

If one or more ~~pumps fail to trip or its associated~~ valves ~~fails~~ fail *to close, the water level may rise up to the top of the condenser pit and reach grade level. If the operator received an alarm from the level sensors, even though the automatic protective features failed, the operator could open the truck entrance door (roll up type door) to allow the flood water to exit the building. If the operator does not receive an alarm, it is assumed that insufficient time will be available for the operator to open the truck door for a CWS break before the water level would effectively cause binding of the door and prevent opening. For TSW breaks, greater than 2 hours is available to open the door.*

If the service building door fails open, the flood rate into the service building could be high enough to flood the service building to a significant level. Since the service building is the main entrance to the plant, personnel would hear or see the flood water and alert operators in the control room. Operator action could then be taken to manually ~~trip the CWS or TSW pumps or~~ close CWS or TSW valves. This is assuming that the level sensors failed but control circuitry for ~~pump trip/~~valve isolation was still available.

If these actions failed, the flood waters would fill up the service building and could potentially enter the control or reactor buildings through several external normally closed watertight doors. On the first floor of the service building there is a watertight door which allows entrance to the reactor building cooling water (RCW) heat exchanger rooms. Failure of this door could allow the flood waters to damage equipment in all three safety divisions and potentially the battery room on the next level. If the watertight door to the RCW rooms does not fail, the water level would rise up in the service building to the next level where there are two watertight doors, one to the battery rooms of the control building and another to the reactor building clean access area. Failure of the watertight door to the battery rooms is assumed to result in core damage as loss of all DC (batteries and battery chargers) will occur. DC power is required for control of safe shutdown systems or to depressurize and use non-safety-related makeup sources such as condensate or AC independent water addition systems. Failure of the watertight door to the *reactor building clean access area could result in damage to all three electrical divisions. If none of these watertight doors fail, flooding could continue to the next level where a ~~normally open~~ watertight door*, normally closed except for routine ingress and egress, *allows access to the control room area. Given the extensive flooding which had occurred to this point, the operators would have sufficient time and warning to* ensure that *~~close~~ this watertight door* is closed*. If the door failed or the operators failed to close it, no core damage should occur because automatic initiation of safety systems such as the high pressure core flooder would ensure that the core remained covered with water. Continued flooding would then reach grade level where the water could exit the service building through the main entrance. It is assumed that failure of any of the external watertight doors (except the control room door) results in core damage.*

Figures 19R-7 and 19R-8 are event trees which describe the turbine building flooding for low and high Power Cycle Heat Sink (PCHS) configurations, respectively. Note that Figure 19R 7 does not apply to STP 3 & 4 because they are a high PCHS design as described in Section 2.4S.1.1. *The accident progression due to a large pipe break in the CWS (the worst case flooding) is described in the event tree. As the CWS break is bounding, no TSW flooding event trees were developed. The success or failure of each flood mitigating feature in the event tree diagram may have a significant impact on the result of accident progression. The event trees in Figures 19R-7 and 19R-8 are described as follows:*

(3) *The bus breaker and/or pump breakers of CWS pumps open and trip all three* operating *pumps ~~(flooding prevention for low PCHS). Although siphoning could occur if the PCHS was higher than the bottom of the condenser pit, the siphon could not cause flooding to grade level. Therefore, the flood would be contained within the turbine building.~~ In case of* the *high PCHS* design of STP 3 & 4, *~~the success probability of~~ this feature is* not credited for turbine building flood mitigation *~~assumed to be zero~~.*

(4) *CWS isolation valves close ~~(flooding prevention for high or low PCHS)~~.*

(8) The control room operator can prevent flood damage to safety-related equipment by manually *~~tripping the CWS pumps or~~* closing the CWS valves. It is assumed that if automatic features failed (given that the sensors did not fail) that control room actuations would also fail. If the sensors failed though, it may be possible to manually close the valves or trip the pumps from the control room once the operator is aware of the flooding condition. The probability of success is higher if the sensors did not fail because the operator would receive two indications of flooding: early in the scenario from the sensors in the turbine building and later from personnel in the service building if the flood were to propagate to that point. In either case, the watertight doors in the control and reactor buildings can prevent damage to safety-related equipment.

~~*The description of flooding for a high PCHS is the same as for a low PCHS except that the pump tripping feature is not credited.*~~

The core damage frequency for turbine building flooding is extremely small for a low PCHS and slightly higher for a high PCHS design of STP 3 & 4.

19R.6.4 Operator Actions

The following site-specific supplement addresses the STP design having all openings to safety-related buildings below flood level closed.

(4) Ensure that the ~~*Close*~~ *watertight door at* the *entrance to the control room area* is closed *if floods in the turbine building result in service building flooding.*

19R.6.6 Conclusions

The following site-specific supplement addresses the STP site being a high PCHS design.

The conclusions from the ABWR probabilistic flooding analysis is that the risk from internal flooding is acceptably low. The estimated core damage frequency from all internal flood sources is very small for a low PCHS and slightly higher for ~~*a*~~ the *high PCHS* design of STP 3 & 4.

19R.7 External Flooding Evaluation

The following site-specific supplement summarizes the external flooding analysis performed for the STP site and addresses departure STP DEP T1 5.0-1.

Summarized in the sections below is the external flooding PRA analyses for the STP 3 & 4 plants. External flooding is defined as intrusion of water from sources outside of plant buildings such that the ability of the plant to achieve safe shutdown is affected. The analysis determined the potential core damage frequency (CDF) that could result from external flooding events for each of the new units and was developed assuming that the watertight door providing normal access to the main control room is open. This assumption provides a conservative and bounding assessment of risk from external flooding because the watertight door to the main control room would be closed except for intermittent ingress and egress (Refer to FSAR Section 2.4S.10).

19R.7.1 Methodology

STP DEP T1 5.0-1

To develop the external flooding analysis for STP 3 & 4, the following steps were performed:

- Identification and screening of external flooding initiating events.
- Quantification of external flooding initiating event frequency.
- Analysis of external flooding accident sequences and development of event trees.
- Quantification of external flooding core damage frequency.

Details of these steps are provided in the subsections that follow.

19R.7.2 Identify and Screen Initiating Events

STP DEP T1 5.0-1

External flooding at the STP site potentially can be initiated by several basic sources: river flooding which includes ice flooding, upstream dam breaks and landslides, tsunamis, rainstorms, and onsite sources including dam breaks and failure of the ultimate heat sink (UHS). Events from these sources could, potentially, be related. For example, a storm could cause both a breach of an upstream dam and local flooding at the site. This analysis considers independent and correlated flooding events.

Ice flooding of the Colorado River adjacent to the STP site is not considered a potential hazard because the warm temperatures of the area and the tidal effects that are felt on the river in the area. Therefore, ice flooding is screened as a potential initiating event.

Based on analysis performed for STP 1&2 (Reference 19R.7-1), landslides are not considered a threat to the STP site. Therefore, landslides are screened as potential external flooding initiating events.

Analysis for STP 1 and 2 (Reference 19R.7-1) also concluded that tsunamis cannot affect the site. Therefore, tsunamis are screened from consideration as initiating events.

The storm surge or seiche resulting from a hurricane could potentially cause flooding at the STP site. However, the maximum water level at the STP site that would be expected from such an event would be elevation 26.74 feet. Since this elevation is below grade level, hurricane storm surge or seiche can be excluded as an external flooding initiating event.

Intense precipitation can result in flooding local to the STP site because plant buildings will be constructed so that all external entrances are at least one foot above the flood level expected from a probable maximum precipitation event. Since the maximum flood level expected from intense precipitation is one foot below grade level for Units 3 and 4, intense local precipitation is screened from consideration as an external flooding initiating event.

The normal operating elevation is 26 feet for the essential cooling pond (ECP) of Units 1 and 2. Since this elevation is below the nominal grade elevation for the STP site, failure of the ECP is excluded as an external flood initiating event.

The cooling tower basin for the UHS contains a large volume of water that, if released, could potentially drain to safety-related buildings on the STP site. However, approximately half of this volume is below grade and, therefore, would not be expected to drain away from the basin. The UHS basin is a cylindrical concrete tank that is surrounded by an earthen berm. The berm extends 3.5 feet above the maximum water level. For water in the UHS basin to reach safety-related buildings, first a failure of the concrete tank must occur, then, the water must erode the earthen berm. It is considered unlikely that any failures of the UHS structure would result in a large rapid release of water. Any failures of the structure would be expected to be small such that site drainage systems would be capable of preventing the water from reaching other safety-related buildings onsite. Therefore, failure of the UHS is screened from further consideration as an external flooding initiating event.

The STP site is located on the Colorado River at river mile 16.4, upstream from the Gulf of Mexico. The potential for dams upstream of the site to cause plant flooding was evaluated as part of the original licensing for Units 1&2. The analyses for Units 1&2 (Reference 19R.7 1) show that a maximum flood level of 32.0 ft MSL is expected at the STP site from a single upstream dam break. Since this level is below the elevation of Unit 3&4 plant buildings, single upstream dam breaks can be screened from further consideration as external flooding initiating events.

In addition the potential flooding effects from multiple, cascading failures of Colorado River dams upstream of the STP site. That analysis shows that a peak still water elevation of 34.1 feet with wave runup to the 43.7 foot elevation. Therefore, multiple, concurrent dam failures are considered as an external flooding initiating event.

The Main Cooling Reservoir (MCR) is formed by a 12.4 mile, earth filled embankment enclosing 7,000 acres of surface area at a normal operating level of 49.0 MSL with a capacity of 175,000 acre feet. The embankment, about 2100 feet south of the south face of the plant power block, rises an average of 40.0 feet above the natural ground surface. Breach of the MCR produces the critical flood levels at the STP site. Therefore, MCR failure is considered as an external flooding initiating event.

19R.7.3 Quantification of External Flooding Initiating Event Frequency

STP DEP T1 5.0-1

The analysis of the frequency for MCR failures begins with the frequency developed as part of the Unit 1&2 IPEEE analysis. That value has been updated to reflect MCR operating experience since completion of the IPEEE. The initiating event frequency for MCR failures that could impact Units 3&4 is determined to be very low.

The frequency of multiple, concurrent upstream dam breaks considers the failure of three dams, the S. W. Freese, Buchanan, and Mansfield Dams. The analysis assumes that the first dam failure can occur randomly and that the second and third failures are dependent on the previous dam failures. The sequence of events analyzed begins with failure of the S. W. Freese Dam which began operation in 1990.

Downstream of the S. W. Freese Dam is the Buchanan Dam. It is assumed that failure of the Buchanan Dam is dependent on the failure of the S. W. Freese Dam. Table 19R-4 gives values for common cause factors. Although not considered a common cause failure in the traditional sense, the second and third dam failures are analyzed using the common cause factors from Table 19R-4. Using the Beta factor from Table 19-4, failure of the Buchanan Dam, given failure of the S. W. Freese Dam is calculated.

Failure of the third dam, the Mansfield Dam, given failure of the first two dams, is calculated using the Gamma factor given in Table 19R-4. The frequency of multiple concurrent dam failures considered as external flooding initiating events is calculated to be very low.

19R.7.4 Accident Sequence Analysis

STP DEP T1 5.0-1

The subsections that follow summarize the accident sequence analysis for the two events considered as external flooding initiating events.

19R.7.4.1 Main Cooling Reservoir Breach

STP DEP T1 5.0-1

Note that this analysis is developed assuming that the watertight door providing normal access to the main control room is open. This assumption provides a conservative and bounding assessment of risk from external flooding because the watertight door to the main control room would be closed except for intermittent ingress and egress (Refer to FSAR Section 2.4S.10).

A breach of the main cooling reservoir could occur suddenly or progress over many minutes. A discussion of previous dam breaches notes that the failure time of most breaches is 15 minutes to one hour from the time of inception to completion of the breach. However, some breaches became fully developed in as little as 6 minutes while others took more than 7 hours. It was also noted that half the breaches identified occurred in less than 1.5 hours. Therefore, it is concluded that, while there is a good deal of uncertainty and variability associated with the breach time, 15 minutes to one hour would likely be conservative. Breach width was also noted to be typically 2 to 5 times dam height (Reference 19R.7-2). The timing of the breach along with the width of the breach affects the height of water that reaches plant buildings. Smaller breaches or breaches that take longer to develop would result in a lower level of water on plant buildings. For smaller and slower-developing breaches, it can be expected that water would not rise above grade elevation on plant buildings. For larger and faster-developing breaches, water level on plant buildings would be higher. The analysis, originally documented in the IPEEE of Units 1&2 (Reference 19R.7-3), considered that failures of the MCR are equally likely to occur anywhere along the perimeter and excluded from consideration that portion of MCR failures that would direct water away from plant buildings. MCR failures that would result in water flowing away from the site would not be considered as external flooding initiating events, consistent with the analysis presented in Reference 19R.7.3. This assumption is considered reasonable since the land around the MRC generally slopes southward towards the Colorado River. This analysis assumed that any breach of the main cooling reservoir that is included in the initiating event definition is sufficiently large that water level will rise above the entrances to plant buildings. This analysis also assumed that the main cooling reservoir breach would cause a loss of offsite power either because of failure of the switchyard equipment or the plant auxiliary transformers that are impacted by the floodwaters. Furthermore, this analysis assumed that the loss of offsite power is not recoverable for several days.

A breach of the main cooling reservoir would cause water to flow across lighted roadways and open areas between the main cooling reservoir and the plant. Security personnel are stationed such that they have a clear view of these areas. On seeing the developing breach or water flow, they would notify the main control room in accordance with their training and procedures.

External access points to the control and reactor buildings are provided with normally-closed, watertight barriers or doors designed to withstand the maximum loadings of any potential main cooling reservoir breach. All these doors are alarmed at the central alarm station so it is unlikely that one would be left open. Failure of any one of these doors would allow water to enter the building and flow through drains, stairways, and non-watertight doors to the essential electrical switchgear rooms below grade. Since there are no internal watertight barriers to protect the rooms on lower elevations from water entering the upper elevations, it is conservatively assumed that failure of one of the watertight doors on the reactor building would result in core damage.

The normal access to the main control building is via the service building through a watertight door on the 2950 mm elevation. As discussed above, this analysis assumes that this door is open. The door is oriented such that water external to the control building will seal the door. In addition, there are other normally-closed watertight doors that provide access to the control building from the service building and that are located either at or below grade. Since the service building is not designed to withstand flooding, it is assumed that a main cooling reservoir breach would result in water entering the service building. If any one of the doors from the service building to the control building is not closed or fails, then water could enter the control building and cause failure of all three divisions of reactor cooling water (RCW) or DC power since these are located below grade. Since there are no internal watertight barriers to protect the rooms below grade in the control building, it is conservatively assumed that failure of one of the watertight doors on the control building would result in core damage.

The turbine building and service building are not designed to withstand the effects of a failure of the main cooling reservoir. Therefore, it is conservatively assumed that any equipment in the turbine building or service building is failed by the flooding caused by a breach of the main cooling reservoir. PRA-related equipment housed in the turbine building includes the condensate and feedwater systems and the combustion turbine generator (CTG).

When notified of a main cooling reservoir breach by security personnel, the operators in the main control room staff would ensure that the normally-open, watertight control room access door is closed. Closing this door prevents water from entering the control building. As discussed above, failure to close this door would result in submerging the control building and is conservatively assumed to result in core damage.

If the door to the main control room is closed, then the event progresses as a loss of offsite power since it is assumed that the MCR breach causes a loss of offsite power Because of the loss of offsite power, all equipment powered from non-essential electrical buses is initially lost. The loss of offsite power would result in the EDGs starting and loading to their respective essential electrical buses. The CTG would be failed by the flood so failure of all three EDGs would result in a station blackout (SBO). For this analysis, a SBO is conservatively assumed to be non-recoverable and result in core damage.

If one or more EDG starts and loads its respective buses, then the reactor can be brought to safe shutdown using equipment powered from the essential AC buses.

The accident progression for this event tree is similar to that of a loss of offsite power. However, for the main cooling reservoir breach, it is assumed that offsite power is not recovered and that failure to insert control rods or a subsequent station blackout would result in core damage.

19R.7.4.2 Multiple, Concurrent Upstream Dam Failures

STP DEP T1 5.0-1

Note that this analysis is developed assuming that the watertight door providing normal access to the main control room is open. This assumption provides a conservative and bounding assessment of risk from external flooding because the watertight door to the main control room would be closed except for intermittent ingress and egress (Refer to FSAR Section 2.4S.10).

The accident progression for multiple, concurrent upstream dam failures is similar to that of the main cooling reservoir breach except for timing. Since the last dam that would fail, the Mansfield Dam, is nearly 300 miles upstream of the STP site, flood waters from that dam failure would not reach the STP site for many hours. In that time, closure of the normally-open main control room access door would be assured. In addition, compensatory actions such as sandbagging or installation of other temporary flood barriers can be installed around access doors. These additional compensatory actions, however, are not quantified as part of this analysis. This analysis also assumes that the flooding that results from multiple, concurrent upstream dam failures will cause a loss of offsite power either because of failure of the switchyard equipment or the plant auxiliary transformers that are impacted by the floodwaters. Furthermore, this analysis assumed that the loss of offsite power is not recoverable for several days.

External access points to the control and reactor buildings are provided with normally-closed, watertight barriers or doors designed to withstand the maximum loadings of any potential main cooling reservoir breach, a more severe event than multiple, concurrent upstream dam failures. All these doors are alarmed at the central alarm station so it is unlikely that one would be left open. Failure of any one of these doors would allow water to enter the building and flow through drains, stairways, and non-watertight doors to the essential electrical switchgear rooms below grade. Since there are no internal watertight barriers to protect the rooms on the lower elevations from water that entered the upper elevations, it is conservatively assumed that failure of one of the watertight doors on the reactor building will result in core damage.

The normal access to the main control building is via the service building through a watertight door on the 2950 mm elevation. In addition, there are other normally-closed watertight doors that provide access to the control building from the service building and that are located either at or below grade. Since the service building is not designed to withstand flooding, it is conservatively assumed that the flooding that results from multiple, concurrent upstream dam failures would result in water entering the service building. If any one of the doors from the service building to the control building fails, then water could enter the control building and cause failure of all three divisions of reactor cooling water (RCW) or DC power since these are located below grade. Since there are no internal watertight barriers to protect the rooms below grade in the control building, it is conservatively assumed that failure of one of the watertight doors on the control building will result in core damage.

The turbine building and service building are not designed to withstand flooding. Therefore, it is conservatively assumed that any equipment in the turbine building or service building is failed by the flooding caused by multiple, concurrent upstream dam failures. PRA-related equipment housed in the turbine building includes the condensate and feedwater systems and the combustion turbine generator (CTG).

When notified of an upstream dam failure, steps will be taken (Refer to Section 19.9.3) to ensure that the watertight main control room access door will be closed prior to flood waters reaching the STP site. Since many hours are available to effect this action and the action is simple and visually verifiable, the probability of failing to ensure closure of the door is considered sufficiently small as to be neglected. Closing this door prevents water from entering the control building.

Since the flooding is assumed to cause a loss of offsite power, all equipment powered from non-essential electrical buses would be lost. The loss of offsite power will result in the EDGs starting and loading to their respective essential electrical buses. The CTG is conservatively assumed failed by the flood so failure of all three EDGs would result in a station blackout (SBO). For this analysis, a SBO is assumed to be non-recoverable and results in core damage.

If one or more EDG starts and loads its respective buses, then the reactor can be brought to safe shutdown using equipment powered from the essential AC buses.

The accident progression for this event tree is similar to that of a loss of offsite power. However, for multiple, concurrent upstream dam failures, it is assumed that offsite power is not recovered and that failure to insert control rods or a subsequent station blackout result in core damage.

19R.7.5 Summary of Accident Sequences

STP DEP T1 5.0-1

The subsections that follow summarize determination of the accident sequences developed for the two events considered as external flooding initiating events. Determination of CDF made use of the existing ABWR PRA logic models and used a process similar to that used to quantify the internal flooding events.

19R.7.5.1 Main Cooling Reservoir Breach Accident

STP DEP T1 5.0-1

Four accident sequences lead to core damage. Core damage results if any one of the top events fails. Development of each of the top events is discussed below.

IEBMCR - Breach of Main Cooling Reservoir
This Initiating Event represents the main cooling reservoir breach. This event is described above.

OCD - Operator Action To Close Control Room Watertight Access Door or RB/CB External Doors Fail

This top event represents failure of the watertight doors to prevent flood waters from entering either the control building or the reactor building. Failure of this top event can occur from two causes. First, the operators can fail to close the normally open, watertight door that provides main control room access from the service building. As described in section above, security personnel are stationed such that they will have a clear view of the area between the main cooling reservoir and plant buildings. This analysis assumes that the security staff is trained and that procedures are in place for them to alert the control room if there are indications of a breach of the main cooling reservoir. Procedures are also assumed to be in place to direct that the main control room access door be closed immediately on notification of a potential external flooding event (Refer to Section 19.9.3). Furthermore, the analysis assumes that the area between the main cooling reservoir and plant buildings is lighted to an extent that any flow of water from a breach of the main cooling reservoir would be clearly visible to the security personnel at night.

As discussed above, development of a main cooling reservoir breach is expected to take from 15 minutes to one hour. Once the security staff notifies the control room of the breach, closing and securing the watertight door takes less than one minute. Therefore, it is assumed that a moderate and adequate amount of time is available to effect the actions to close the control room access door. Then the failure probability for this event was assigned using the values in Table 19R-4.

Even if operator action to close the normally-open door is successful, failure of any one of the watertight doors that allow access to the reactor building or control building could randomly fail. Using the values in Table 19R-4, the probability of random door failures that allow water to enter either the control building or the reactor building was calculated.

The total probability of failing to isolate the control and reactor buildings from a main cooling reservoir breach is the sum of the operator failure probability and the random door failure probability.

C - Failure To Insert Control Rods

This top event represents failure to insert the control rods on the loss of offsite power caused by the external flooding event. The probability of this event is taken from the internal events PRA models.

PO1 - SRVs Fail To Open (After Scram)

This top event represents failure of the safety relief valves (SRVs) to open after a reactor trip. The probability of this event is taken from the internal events PRA models.

SSD - Reactor Brought To Safe Shutdown Condition

This top event represents failure to bring the reactor to a safe shutdown condition. Since the main cooling reservoir breach is assumed to result in a non-recoverable loss of offsite power, this node is quantified using the existing TEO event tree sequences but accounting for the additional failures that would be caused by the flooding. Basic events that represent these additional failures were set to “True” for the quantification.

The 11 core damage sequences from TEO were quantified to produce the conditional probability of core damage given that an external flooding event occurred. The resulting probability is determined to be low.

Since failure of each of the top nodes on the IEBMCR event tree results in core damage and since each of the top nodes is independent of the others, the total CDF for a main cooling reservoir breach is the product of the initiating event frequency, the success probability of any previous nodes, and the top node failure probability. The total CDF for a breach of the main cooling reservoir is determined to be very low.

19R.7.5.2 Multiple, Concurrent Upstream Dam Failures Accident

STP DEP T1 5.0-1

Four accident sequences lead to core damage. Core damage results if any one of the top events fails. Development of each of the top events is discussed below.

IEDAM - Multiple Concurrent Upstream Dam Failures
This top event represents the failure of the three dams upstream of the STP site on the Colorado River. This event is described above.

WTDOOR - Reactor Building and Control Building External Watertight Doors Fail
This top event represents failure of the watertight doors to prevent flood waters from entering either the control building or the reactor building. Because of the long time available for notification and action following failure of the last dam on the Colorado River, it is assumed that the failure probability of operator action to close the normally-open watertight door to the main control room can be neglected.

Any one of the nine watertight doors that allow access to the reactor building or control building could randomly fail. Using the values in Table 19R-4, the probability of random door failures that allow water to enter either the control building or the reactor building is calculated.

C - Failure To Insert Control Rods
This top event represents failure to insert the control rods on the loss of offsite power caused by the external flooding event. The probability of this event is taken from the internal events PRA models.

PO1 - SRVs Fail To Open (After Scram)

This top event represents failure of the safety relief valves (SRVs) to open after a reactor trip. The probability of this event is taken from the internal events PRA models.

SSD - Reactor Brought To Safe Shutdown Condition

This top event represents failure to bring the reactor to a safe shutdown condition. This top event is described in Section 19R.7S.5.1.

Since failure of each of the top nodes on the IEDAM event tree results in core damage and since each of the top nodes is independent of the others, the total CDF for an external flooding event caused by multiple, concurrent upstream dam failures is the product of the initiating event frequency, the success probability of any previous nodes, and the top node failure probability. The total CDF for a breach of the main cooling reservoir is determined to be very low.

19R.7.5.3 Total External Flooding Event CDF

STP DEP T1 5.0-1

The total CDF from external flooding events is obtained by summing the CDF from each of the events above and is determined to be very low.

19R.7.6 Important External Flooding-Related Design Features

STP DEP T1 5.0-1

There are several design features important to minimizing external flood-related risk. One is that all buildings are constructed with entrances at least one foot above the flood level that would result from a PMP related flood. This feature allows screening of most external flooding events. Another feature is that all plant entrances and penetrations located below the maximum flood level are protected by watertight barriers or doors. Also, a clear view is provided from plant buildings to the main cooling reservoir thereby allowing for timely notification to the main control room of a main cooling reservoir breach.

19R.7.7 Operator Actions Related to External Flooding

STP DEP T1 5.0-1

One operator action is important to external flooding risk. This action, timely closure of the watertight door at the entrance to the main control room is similar to the event included in section 19R.6.4. However, the cues to initiate the action for external flooding events are different than for internal flooding.

19R.7.8 External Flooding Reliability Goals (Input to RAP)

STP DEP T1 5.0-1

The results of the external flooding analysis show that watertight doors are important to reducing external flood-related risk. Watertight doors are included as input to the RAP because of internal flooding events. The information from Section 19R.6.5 related to watertight doors is also applicable to external flooding events and is applied to all external watertight doors on the reactor and control buildings.

19R.7.9 Conclusions

STP DEP T1 5.0-1

The conclusions from the ABWR probabilistic external flooding analysis are that the risk from external flooding is acceptably low, even with the conservative assumption that the watertight normal access door to the control room is open. The risk from external flooding would be significantly lower if analyzed assuming that the door is closed, as described in FSAR Section 2.4S.10. It is also concluded that the incremental risk from external flooding events is within the goals for an increase in CDF or LERF.

19R.8 References

The following site-specific supplement provides references.

19R-1 STPEGS 1&2 UFSAR Section 2.4, Hydrologic Engineering, Revision 13.

19R-2 "Prediction of Embankment Dam Breach Parameters," DSO-98-004, Dam Safety Office, Water Resources Research Laboratory, US Department of the Interior, Bureau of the Interior, July, 1998.

19R-3 South Texas Project Electric Generating Station Level 2 Probabilistic Safety Assessment and Individual Plant Examination, Revision 0.

Table 19R-6 Internal Flooding Core Damage Frequency (CDF)

The following site-specific supplement states that low PCHS is not applicable to STP 3 & 4.

	CDF (per reactor year)	
Building	**Low PCHS***	**High PCHS***
Turbine	Not Applicable	
Control	Not Applicable	
Reactor	Not Applicable	
Total	Not Applicable	

* Not part of DCD (refer to SSAR).

Figure 19R-6 removed by NRC staff
Offical Use Only - Security Related Information

Figure 19R-6 Reactor Building Arrangement - Elevation 12300 mm (1F)

Figure 19R-7 Turbine Building Flooding (Low PCHS)

The information in this figure is incorporated as a site-specific supplement to the reference ABWR DCD.

Note that this figure does not apply to the high PCHS design of STP 3 & 4. This figure is deleted.