Maria Korsnick
Site Vice President

R.E. Ginna Nuclear Power Plant, LLC
1503 Lake Road
Ontario, New York 14519-9364
585.771.3494
585.771.3943 Fax
maria.korsnick@costellation.com

Constellation Energy
Generation Group

September 29, 2006

U. S. Nuclear Regulatory Commission
Washington, DC 20555

ATTENTION: Document Control Desk

SUBJECT: **R.E. Ginna Nuclear Power Plant**
Docket No. 50-244

License Amendment Request: Change to Technical Specification 3.7.8, Service Water (SW) from an Electrical Train Based to a Pump Based Specification

In accordance with the provisions of 10 CFR 50.90, R.E. Ginna Nuclear Power Plant, LLC (Ginna LLC) is submitting a request for an amendment to change Technical Specification (TS) 3.7.8 from an electrical train based specification to a pump based specification. This is a risk informed submittal.

Ginna has a total of four service water (SW) pumps, with two pumps powered from each safeguards power supply. Operability of the system is defined by the train, and the TS Bases defines a train as one pump from each train (power supply). Currently, the accident analysis indicates that one SW pump is sufficient for post accident operations. However, analysis performed for the planned Extended Power Uprate (EPU) indicates that two SW pumps will be required for post-accident operations. Ginna has determined that the attached amendment provides the best long term solution by ensuring sufficient SW pump capacity is available for post-accident operations, while providing reasonable LCO action times for unplanned and scheduled maintenance. As an interim measure, a change to the TS Bases requiring both pumps in the electrical train to be operable for the train to be considered operable will be initiated for post EPU operations until this amendment is approved.

Both technical analyses and risk insights were used to determine the acceptability of this proposed change. The technical analysis, contained in Attachment (1), provides results that show the availability of adequate SW for the Design Basis Accident (DBA). The risk insights, contained in Attachment (2), show that the likelihood of core damage resulting from this change is significantly below regulatory guidance provided in Regulatory Guides 1.174 and 1.177. The

A001

1001633

large early release frequency impact, although not explicitly calculated, is extremely small. Therefore, we find the proposed change acceptable.

We have considered the possibility of a significant hazard associated with this proposed change and have determined that there are none. We have also determined that operation with the proposed change would not result in any significant change in the types or amounts of any effluents that may be released offsite, nor would it result in any significant increase in individual or cumulative occupational radiation exposure. Therefore, the proposed change is eligible for categorical exclusion as set forth in 10 CFR 51.22(c)(9). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment is needed in connection with the proposed amendment.

This proposed change to the Technical Specifications (Attachment 3) and our determination of significant hazards have been reviewed by our Plant Operation Review Committee (PORC) and Nuclear Safety Review Board (NSRB), and they have concluded that implementation of these changes will not result in an undue risk to the health and safety of the public.

We request that this change be approved by March 30, 2007, with the amendment being implemented within 60 days of issuance. As noted above, we believe that this change will assure the SW system will remain available to perform its safety function while maintaining a reasonable opportunity to correct situations that may arise during operation.

Should you have questions regarding the information in this submittal, please contact Mr. Robert Randall at (585) 771-3734 or Robert.Randall@constellation.com.

Very truly yours,

Mary G. Korsnick

Mary G. Korsnick

STATE OF NEW YORK :
: **TO WIT:**
COUNTY OF WAYNE :

I, Mary G. Korsnick, begin duly sworn, state that I am Vice President, R.E. Ginna Nuclear Power Plant, LLC (Ginna LLC), and that I am duly authorized to execute and file this request on behalf of Ginna LLC. To the best of my knowledge and belief, the statements contained in this document are true and correct. To the extent that these statements are not based on my personal knowledge, they are based upon information provided by other Ginna LLC employees and/or consultants. Such information has been reviewed in accordance with company practice and I believe it to be reliable.

Mary G. Korsnick

Subscribed and sworn before me, a Notary Public in and for the State of New York and County of Monroe, this 29 day of September, 2006.

WITNESS my Hand and Notarial Seal: Sharon L. Miller
Notary Public

My Commission Expires: 12-21-06
Date

SHARON L. MILLER
Notary Public, State of New York
Registration No. 01MI6017755
Monroe County
Commission Expires December 21, 2006

MK/MR

Attachments: (1) Evaluation of Proposed Change
(2) Risk Insights
(3) Proposed Technical Specification Changes (mark-up)

cc: S. J. Collins, NRC
P.D. Milano, NRC
Resident Inspector, NRC (Ginna)
P.D. Eddy, NYSDPS
J. P. Spath, NYSERDA

Attachment (1)

Evaluation of Proposed Changes

Attachment (1)

Evaluation of Proposed Change

1. DESCRIPTION

This letter is a request to amend Operating License No. DPR-18 for the R. E. Ginna Nuclear Power Plant (Ginna) to change Technical Specification (TS) section 3.7.8 from electrical train based to a component based TS.

2. PROPOSED CHANGE

This proposed change would modify TS section 3.7.8 to require a specific number of Service Water (SW) pumps to be operable, rather than specific trains as exists in the current specification. Currently TS 3.7.8 requires two SW trains to be operable. The trains are defined by the pump(s) electrical power supply in the TS Bases. If one train is inoperable the plant enters a 72 hour Allowed Outage Time (AOT). The proposed change would modify TS 3.7.8 to require all four pumps to be operable. With one pump inoperable the plant would enter a 14 day AOT. If two of the four pumps were inoperable, the plant would enter a 72 hour AOT. Emergency power supply availability is considered by the relationship of TS 3.7.8 with TS 3.8.1, AC Sources – Modes 1, 2, 3, and 4, providing for a 4 hour AOT in the event of the redundant component emergency power supply being inoperable. Surveillance Requirement (SR) 3.7.8.2 will also be modified to remove the reference to "train" for consistency in wording.

3. BACKGROUND

Ginna's SW specification currently requires 2 trains to be operable. With one train inoperable the plant is in a 72 hour AOT. The bases currently defines the trains by electrical power supply to the pumps, with the A & C pumps in one train and the B & D pumps in the opposite train. All four pumps (both trains) supply a single common SW loop header. A train is currently considered operable with one of two pumps in that train operable. Since the flow loops are operated in a cross-connected configuration, TS addresses them as a single loop which carries its own action statement.

Currently, Ginna could operate indefinitely with one SW pump in each train (two pumps total) out of service and not enter a LCO action statement. Considering a Loss of Coolant Accident (LOCA) with a loss of off-site power and the worst single failure being a Diesel Generator (DG) failure, one SW pump would be available for post LOCA recovery operations. At the current licensed power level, one SW pump is sufficient to remove the existing heat loads from the containment atmosphere and sump in the recirculation phase of a LOCA. However, analysis performed for Ginna's extended power uprate (EPU) indicates that after EPU, with maximum design lake temperature, one service water pump is not sufficient due to reduced flow from potential flashing downstream of the containment fan coolers. Local operator action to isolate the non functioning fan coolers (those powered from the failed DG) could mitigate this effect. However, these operator actions would be in a high radiation area causing unnecessary dose,

expend operational resources, and although technically justifiable are not considered acceptable by Ginna management. With two available SW pumps, these operator actions are not required. Therefore, Ginna is proposing that the TS section 3.7.8 be modified to require all four SW pumps be operable, with a decreasing AOT as the number of operable pumps decrease. Ginna has determined that the changes discussed in this amendment request will provide the necessary operational flexibility for unexpected equipment failures while ensuring adequate equipment redundancy and safety margins for continued operation.

As an interim measure (i.e., from the time the EPU is implemented until the new TS is in place), Ginna will initiate a TS Bases change per TS 5.5.13, TS Bases Control Program, requiring both pumps in an electrical train to be operable for that train to be considered operable. This will ensure that two SW pumps are available for post accident operations.

4. TECHNICAL ANALYSIS

The function of the SW System is to provide a heat sink for the removal of process and operating heat from safety related components during a Design Basis Accident (DBA) or transient. During normal operation, and a normal shutdown, the SW System also provides this function for various safety related and non-safety related components.

The design basis of the SW System is, in conjunction with a 100% capacity containment cooling system, to provide for heat removal following a main steam line break (MSLB) inside containment to ensure containment integrity. The SW System is also designed to perform containment cooling via the Containment Recirculation Fan Coolers (CRFC) during both the injection phase and recirculation phase of a design basis LOCA. In addition, during the recirculation phase of a design basis LOCA, the SW System in conjunction with the CCW system and a 100% capacity Emergency Core Cooling System (ECCS) provides long term cooling of the reactor by cooling recirculated water from the containment sump. This prevents the containment sump fluid from increasing in temperature during the recirculation phase following a LOCA and provides for a gradual reduction in the temperature of this fluid as it is re-circulated to the Reactor Coolant System (RCS) by the ECCS pumps. SW must be shared between several loads. Most notably, during the recirculation phase of a design basis LOCA the SW flow must be increased to the CCW Heat Exchangers to an amount greater than the normal at power flow to facilitate sump water heat removal. Prior to EPU one SW pump has the capacity to provide this required flow while maintaining adequate flow to the CRFC. Given Ginna's current definition of a train, only one SW pump must be operable for that train to be operable. Therefore, even with the assumption of a loss of off site power and the single failure of one DG in conjunction with a LOCA, the current TS is adequate to assure the minimum SW flow for post accident operations.

Combined References 8.a, 8.b and 8.c (previously accepted by the NRC as part of Ginna's EPU submittal) indicate that one operating SW pump remains acceptable for the MSLB and the injection phase of the LOCA. However, two operating SW pumps are required to remove the necessary heat loads during the recirculation phase of a large break LOCA after EPU. Assuming a single failure of a DG, a single SW pump will no longer be sufficient to provide the adequate SW flow to the CRFCs after increasing flow to the CCW Heat Exchangers. Therefore the

current TS with a train operability defined as one pump operable is no longer acceptable. As described below, the proposed amendment is the best option to assure adequate SW capacity for post accident operations after EPU.

The proposed change will be an improvement in operational safety and flexibility. The proposed amendment establishes the appropriate AOT to ensure adequate service water pumps are available for post accident recovery operations without those additional operator actions. With this proposal, Ginna will be in a 14 day AOT with any one SW pump inoperable, a 72 hour AOT with any two pumps inoperable, and TS 3.0.3 with three pumps inoperable. This is a decrease in AOT for three of the four possible pump inoperability combinations. Table 1 below illustrates the conservatism inherent in the proposed amendment as compared to the existing TS.

Table 1
Comparison of Action Statements
Existing vs. Proposed TS

Number of Inoperable SW Pumps	AOT (Existing TS)	AOT (Proposed TS)
1	Indefinite	14 Days
2 Opposite Electrical Trains	Indefinite	72 Hours
2 Same Electrical Train	72 Hours	72 Hours
3	72 Hours	6 Hours (LCO 3.0.3)

As discussed above, a change to the TS Bases requiring both pumps in the electrical train to be operable for the train to be considered operable will be initiated for post EPU operations. Although this option will be implemented on an interim basis, and assures that the required number of SW pumps will be available for post accident operations, it is unnecessarily restrictive and is not consistent with current industry standards for single failure criteria. That is, if one train of a redundant safety-related fluid system or its safety supporting systems is temporarily rendered inoperable due to short term maintenance as allowed by the unit technical specifications, a single failure need not be assumed in the other train. If a SW pump is already

inoperable and an LCO is controlling its allowed outage time, then another failure (typically considered to be a DG failure) need not be considered. Under these interim requirements, two pumps out of service (one in each train) places the plant in LCO 3.0.3, even though sufficient SW is available for accident mitigation within the accident analysis.

As can be seen from Table 2 below, moving from this interim configuration to the proposed TS is not conservative in all respects and must be evaluated for the risk associated with increasing the AOT for the two configurations where the AOT increases. This risk was evaluated in Attachment 2 and found to be acceptable.

Table 2
Comparison of Action Statements
Existing TS (After Bases Change) vs. Proposed TS

Number of Inoperable SW Pumps	AOT Existing TS – After Interim Bases Change	AOT - Proposed TS
1	72 Hours	14 Days
2 Opposite Electrical Trains	6 Hours (Both Trains Considered Inoperable - LCO 3.0.3)	72 Hours
2 Same Electrical Train	72 Hours	72 Hours
3	6 Hours (LCO 3.0.3)	6 Hours (LCO 3.0.3)

In order to evaluate the proposed TS change it is also necessary to evaluate the aspect of power supply availability. The accident analysis assumes a loss of off-site power separate from the single failure criteria. Because an inoperable DG is assumed to be the single failure, and a loss of offsite power is assumed to occur apart from the single failure criteria, safeguards equipment associated with the inoperable DG is not assumed to operate following a DBA. Therefore, additional inoperable equipment associated with the operable DG places the plant outside of the accident analysis assumptions. To avoid operation in this condition Ginna TS section 3.8.1 (AC Sources – Modes 1, 2, 3, and 4) required action B.2 (One DG Inoperable) states, "Declare

required feature(s) supported by the inoperable DG inoperable when its required redundant feature(s) is inoperable." With those criteria in mind, Ginna has analyzed the proposed change to TS 3.7.8 considering the possible different SW pump and DG operability configurations, and the TS required action for those configurations. The results, shown in Table 3, demonstrate that with the proposed change, the available number of SW pumps remains within the assumptions provided in the accident analysis. If not, timely action is taken to place the plant in a safe mode.

Table 3
SW Pump Inoperability Matrix for the Proposed TS

Condition	Inoperable SW Pump(s)*	Inoperable Diesel Generator	Applicable LCO(s) and Actions
1	Any 1/4	None	3.7.8 A.1 –14 Day Shutdown
2	Any 2/4	None	3.7.8 B.1 – 72 Hour Shutdown
3	Any 3/4	None	3.7.8 D.1 – Enter LCO 3.0.3 Immediately
4	A or C	A	3.7.8 A.1 – 14 Day Shutdown 3.8.1 B.4 – 7 Day Shutdown
5	A or C	B	3.7.8 A.1 –14 Day Shutdown 3.8.1 B.2 – 4 Hours Declare SW Pumps B & D Inoperable then enter 3.7.8 D.1 – Enter LCO 3.0.3 Immediately
6	B or D	A	3.7.8 A.1 –14 Day Shutdown 3.8.1 B.2 – 4 Hours Declare SW Pumps A & C Inoperable, then enter 3.7.8 D.1 – Enter LCO 3.0.3 Immediately

7	B or D	B	3.7.8 A.1 – 14 Day Shutdown 3.8.1 B.4 – 7 Day Shutdown
8	A and C	A	3.7.8 B.1 – 72 Hour Shutdown 3.8.1 B.4 – 7 Day Shutdown
9	A and C	B	3.7.8 B.1 – 72 Hour Shutdown 3.8.1 B.2 – 4 Hours Declare SW Pumps B & D Inoperable, then enter 3.7.8 D.1 - Enter LCO 3.0.3 Immediately
10	B and D	A	3.7.8 B.1 – 72 Hour shutdown 3.8.1 B.2 – 4 Hours Declare SW Pumps A & C Inoperable, then 3.7.8 D.1 – Enter LCO 3.0.3 Immediately
11	B and D	B	3.7.8 B.1 – 72 Hour shutdown 3.8.1 B.4 – 7 Day Shutdown
12	[A or C] and [B or D] i.e. one from each electrical train	A or B	3.7.8 B.1 – 72 Hour shutdown 3.8.1 B.2 – 4 Hours Declare Remaining SW Pump from affected DG bus inoperable, then 3.7.8 D.1 – Enter LCO 3.0.3 Immediately

*A and C SW Pumps – Powered from Bus 18 (A DG)

*B and D SW Pumps – Powered from Bus 17 (B DG)

Regarding the change to SR 3.7.8.2, the loop header is cross connected and is considered a common header, and the specific valves being verified in their correct position will not change. Therefore, removing the reference to train from SR 3.7.8.2 has no impact on the meaning of the requirement, and only serves to maintain consistency and avoid confusion.

Risk Insights

Ginna has evaluated the risk consequences of the proposed change per References 8.d and 8.e, and found them to be acceptable. This evaluation is described in Attachment (2). It should be noted that Ginna originally evaluated this submittal for a 31 day AOT for one SW pump out of service and obtained acceptable results. However, to be conservative and consistent with similar AOTs throughout the industry, an AOT of 14 days is being requested.

Summary

The technical evaluation demonstrates that the required number of SW pumps will be available at all times given single failure criteria, or immediate action will be taken to place the plant in a safe mode. Emergency power availability to the operable pumps is also considered. The proposed AOTs are reasonable, and the risk evaluation demonstrates that the associated risk is within the acceptable limits of established regulatory guidance. Therefore, the change will insure safety by providing timely action to restore inoperable pumps when the margin to the minimum required number of pumps decreases.

5. NO SIGNIFICANT HAZARDS DETERMINATION

R.E. Ginna Nuclear Power Plant, LLC has evaluated whether or not a significant hazards consideration is involved with the proposed amendment by focusing on the three standards set forth in 10 CFR 50.92, "Issuance of amendment," as discussed below:

1. Does the proposed change involve a significant increase in the probability or consequences of an accident previously evaluated?

Response: No.

The safety related function of the Service Water (SW) System is to provide cooling for safety related equipment, mitigate the containment response effects of a Main Steam Line Break (MSLB) and design basis Loss of Coolant Accident (LOCA), and provide long term containment and core cooling in the event of a LOCA. The operation of the SW system, including the number of pumps operating or available, has no affect on the probability of these accidents.

The probability of a loss of SW event is not increased. The proposed TS provides for more restrictive actions for pump inoperability than the existing TS, thereby reducing the probability of this event.

The consequences of a MSLB or LOCA or other design basis accidents are not increased beyond that assumed in the accident analysis. Two service water pumps are sufficient for all accident mitigation functions. The change provides for adequate service water supply (2 pumps) for both normal and accident conditions. The availability of associated power supplies is also considered. For a reduction in the total number of available pumps, appropriate LCO action statements ensure that the pumps are returned to service within a time limit commensurate with an acceptable level of plant safety and risk, or the plant is placed in a safe mode.

The loss of SW has been previously evaluated and measures implemented to mitigate the event. Since a loss of SW assumes no SW pumps are operating, the proposed amendment has no affect on consequences of this event.

Therefore, the proposed change does not involve a significant increase in the probability or consequences of an accident previously evaluated.

2. Does the proposed change create the possibility of a new or different kind of accident from any accident previously evaluated?

Response: No.

The only accidents directly initiated from this system are the loss of SW or flooding concerns. Both of these accidents have been previously evaluated with acceptable results. Therefore, this change does not create the possibility of a new or different type of accident from any accident previously evaluated.

3. Does the proposed change involve a significant reduction in a margin of safety?

Response: No.

This change will ensure that sufficient SW pumps are available for accident mitigation at any one time while still providing the appropriate operational flexibility. A risk determination demonstrates that any increase in risk associated with this change is within the established regulatory guidelines. The technical analysis shows that appropriate action statements exist to ensure adequate SW is available for accident mitigation, considering emergency power supply availability. Therefore, this proposed change does not involve a significant reduction in the margin of safety.

Based on the above, R.E. Ginna Nuclear Power Plant, LLC concludes that the proposed amendment(s) present no significant hazards consideration under the standards set forth in 10 CFR 50.92(c), and, accordingly, a finding of "no significant hazards consideration" is justified.

In conclusion, based on the considerations discussed above, (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner,

(2) such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendment will not be inimical to the common defense and security or to the health and safety of the public.

6. ENVIRONMENTAL ASSESSMENT

A review has determined that the proposed amendment would change a requirement with respect to installation or use of a facility component located within the restricted area, as defined in 10 CFR 20, or would change an inspection or surveillance requirement. However, the proposed amendment does not involve (i) a significant hazards consideration, (ii) a significant change in the types or significant increase in the amounts of any effluent that may be released offsite, or (iii) a significant increase in individual or cumulative occupational radiation exposure. Accordingly, the proposed amendment meets the eligibility criterion for categorical exclusion set forth in 10 CFR 51.22(c) (9). Therefore, pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the proposed amendment.

7. PRECEDENT

Point Beach has a pump based TS similar to the proposed change.

Indian Point Units 2 & 3 have pump based TS, although the pumps are divided between essential and non-essential headers.

8. REFERENCES

a. Westinghouse Calc Note CN-CRA-04-74, Ginna GOTHIC Containment Model for LOCA and MSLB Analysis

b. Westinghouse Calc Note CN-CRA-04-80, Ginna Extended Power Uprate Project: Containment Response to the MSLB Event

c. Westinghouse Calc Note CN-CRA-04-55, Ginna Extended Power Uprate Project: LOCA Long-Term Mass and Energy Release and Containment Integrity Analysis

d. Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis

e. Regulatory Guide 1.177, An Approach for Plant-Specific, Risk Informed Decision Making: Technical Specifications

9. REGULATORY COMMITMENTS

None

Attachment (2)

Risk Insights

Attachment (2)

Risk Insights

1.0 Probabilistic Assessment of the Proposed Service Water Required Action Completion Time Extension

To assess the overall impact of the proposed amendment on plant safety a plant specific analysis has been performed to quantify the change in risk. The risk evaluation was performed using the three-tiered approach suggested in RG 1.177, as follows:

Tier 1	PSA Capability and Insights
Tier 2	Avoidance of Risk-Significant Plant Configurations
Tier 3	Risk-Informed Configuration Risk Management

Evaluations for each of these tiers are provided below.

1.1 Tier 1, Analysis of Risk

Tier 1 is an evaluation of the impact on plant risk of the proposed Technical Specification change as expressed by the change in the following metrics:

CDF	core damage frequency
ICCDP	incremental conditional change in core damage probability
LERF	large early release frequency
ICLERP	incremental conditional large early release probability

These metrics are evaluated in this section using the service water (SW) pump data discussed below.

1.1.1 Service Water System Data used in Analysis of Risk

This subsection discusses the SW unavailability, reliability, and common cause data used in the analysis of the proposed required action completion time extension.

1.1.1.1 Service Water Unavailability Data

The baseline CDF and LERF terms refer to the average risk measures calculated using historical average equipment unavailability. These values are shown in Table 1 for the four SW pumps, including the motors.

Table 1
Best Estimate Service Water System Unavailabilities
(Does not Include Support System Unavailability)

Service Water Pump	Unavailability At-power for dedicated unit			
	Pre-AOT Extension (PSA Values)	Current MR Performance Criteria	Post-AOT Extension (PSA Values)	Post-AOT MR Performance Criteria
A	356 hours per year	<1471 hours per 2 cycles	356 hours per year	<1471 hours per 2 cycles
B	293 hours per year	<1471 hours per 2 cycles	293 hours per year	<1471 hours per 2 cycles
C	138 hours per year	<1471 hours per 2 cycles	138 hours per year	<1471 hours per 2 cycles
D	234 hours per year	<1471 hours per 2 cycles	234 hours per year	<1471 hours per 2 cycles

AOT = Allowed Outage Time

A review of the historical unavailability of the SW pumps for the four year data window used to develop the above data indicates that all but 78.3 hours (or 2.1%) of SW pump unavailability occurred while the plant was on line. Further, the entire 78.3 hours was unplanned maintenance, such that all planned maintenance of the SW pumps occurred on-line. This is due to the fact that the current Technical Specification allows a single SW pump to be removed from service indefinitely, provided the other pump powered by the same electrical train is operable, such that scheduled maintenance (as well as most corrective maintenance) is performed on-line. Since all planned maintenance is currently performed on-line, no increase in on-line SW pump unavailability is planned or anticipated (i.e., there is no planned maintenance that is currently being performed during outages which will now be performed on-line). This is reflected in Table 1. Additionally, it is anticipated that future unavailability will not increase, given the new limit on out of service time for a single pump while on line.

The Maintenance Rule (MR) unavailability performance criteria will remain at their current level, which will maintain the current limit on SW pump unavailability. An analysis was performed to ensure that the existing MR unavailability performance criteria are adequate to preclude any significant increase in plant risk above historical levels. This was done by setting all the SW pumps to their MR unavailability performance criteria concurrently. This represents an increase in unavailability of between approximately 60% (for the A pump) and 420% (for the C pump). The CDF using the MR limits was compared to the CDF using historical average unavailability values. The result of this very conservative analysis shows

an increase in plant risk of 1.2E-06/yr. As discussed above, the actual unavailabilities are not expected to increase over historical values.

1.1.1.2 Service Water Pump Reliability Data

The SW pumps and motors are modeled as a single component. Two failure modes are modeled as shown in Table 2. Interfacing system and components are modeled separately.

Table 2
Service Water Pump Reliability

Failure Mode	Mean Failure Rate	Bases
Failure to Start	2.834E-03 per demand	The prior distributions are based on generic industry data from several sources. These prior distributions were Bayesian updated with plant experience from the four SW pumps from 1980-1988 and 1994-2000.
Failure to Run	1.063E-05 per hour	

SW pump failure data from 2001 through June of 2006 was reviewed to ensure that recent operating experience has not shown a significant increase in failures. This data indicates one failure to start during the 5.5 year period. Conservatively assuming 26 starts per pump per year (the running pumps are alternated every two weeks), the most recent plant data equates to a failure to start rate of:

1 failure/(4 pumps * 26 demands/yr * 5.5 yr) = 1.75E-03/demand

The data also indicates one failure to run during the period. Again, using a conservative assumption that each pump runs for half the year (there are typically two pumps running, with three pumps running during the hot weather months), this data equates to a failure to run rate of:

1 failure/(4 pumps * 8760 hours/yr * 0.5 * 5.5yr) = 1.04E-05/hour.

Both of these values are in close agreement with the failure rates used in the analysis and do not indicate any significant increase in failure rates.

1.1.1.3 Service Water Pump Common Cause Data

The SW pump common cause factors are taken directly from NUREG/CR-5497, Common Cause Failure Parameter Estimations. The failure to start factors are taken from NUREG/CR-5497, Table 10-1, while the failure to run factors are taken from Table 10-4. These are shown below:

Table 3
Service Water Pump Common Cause Data

Group	Factor	Fail-to-Start	Fail-to-Run
PSW01A, PSW01B, PSW01C, PSW01D	α1	0.9228	0.9623
	α2	0.0620	0.0161
	α3	0.00847	0.00549
	α4	0.00674	0.0161

1.1.2 Change in Average Risk

RG 1.174 provides acceptance criteria for the change in CDF and LERF. The criteria are conditional on the value of the baseline risk metric in that if the CDF is considerably higher than 1.0E-04 per reactor year then the focus should be on finding ways to decrease rather than increase it. The Ginna PSA (GPSA) Revision 6.2 has a calculated internal and external event CDF of less than 1.0E-04 per reactor year. Given this baseline CDF, the guidance considers increases in CDF and LERF that are less than 1.0E-06 and 1.0E-07 respectively as very small.

The change in average risk resulting from the proposed AOT extension was evaluated by comparing the risk using the current SW pump unavailabilities against the risk using the anticipated SW pump unavailabilities with the new AOTs. However, as discussed in Section 1.1.1.1, above, the SW pump unavailabilities with the new AOTs are expected to be no more than the current unavailabilities, and are likely to be less. As such, there is no increase in average risk, and the criteria in RG 1.174 for both CDF and LERF are met.

1.1.3 Change in ICCDP and ICLERP

RG 1.177 provides acceptance criteria for ICCDP and ICLERP. The purpose of the numerical guidelines is to demonstrate that the risk increase is small and to provide a quantitative basis for the risk increase based on the aspects of the Technical Specification change modeled. A small risk increase is defined as ICCDP less than 5.0E-07 and ICLERP less than 5.0E-08.

ICCDP and ICLERP are defined numerically as:

ICCDP = [(conditional CDF with the subject equipment out of service)
– (baseline CDF with nominal expected equipment unavailabilities)]

* (duration of single required action completion time under consideration)

ICLERP = [(conditional LERF with the subject equipment out of service)
– (baseline LERF with nominal expected equipment unavailabilities)]
* (duration of single required action completion time under consideration)

As compared to the existing Technical Specification AOTs for the Service Water system, the proposed AOTs are all either equally restrictive or more restrictive. That is, for a single SW pump out of service, or two SW pumps powered from opposite electrical trains out of service (i.e., pumps A and B, A and D, B and C, or C and D), the current AOT has no limit on the out of service time, while the proposed AOT would limit the out of service time to 14 days for a single pump and 72 hours for two pumps. For two SW pumps powered from the same electrical train (i.e., pumps A and C, or B and D) both the current AOT and the proposed AOT would limit the out of service time to 72 hours. Thus, as compared to the existing Technical Specifications, the proposed change would be risk beneficial from a conditional CDF and LERF standpoint.

However, at post-EPU conditions a single SW pump is not considered capable of providing adequate flow to the containment recirculation fan coolers (CRFCs) during sump recirculation following a LOCA with a loss of offsite power and a single active failure. The potential exists for flashing of the service water in the outlet piping downstream of the operating CRFCs, which could prevent flow through the coolers. This would prevent adequate containment heat removal. For the sole purpose of ensuring that two SW pumps are available to provide adequate flow to the CRFCs following a LOCA with a loss of offsite power and a single active failure, the Technical Specification basis for the service water system will need to be changed prior to the EPU to require two SW pumps to be operable in order for a SW pump train to be operable. Since the failure of containment heat removal due to flashing of the service water in the outlet piping downstream of the operating CRFCs creates the potential for increased risk in an otherwise risk beneficial Technical Specification change, this evaluation of the conditional CDF and LERF will address the additional risk associated with operating with one or two SW pumps out of service (and the remaining equipment at nominal expected unavailabilities) as it relates to this containment heat removal issue.

With the change to the existing Technical Specification basis (i.e., an operable SW pump train requires two operable pumps), a single SW pump could be out of service for 72 hours, while the proposed AOT would allow 14 days. Thus an ICCDP and ICLERP must be calculated for these cases. Also, after the basis change, two SW pumps powered from opposite electrical trains (i.e., pumps A and B, A and D, B and C, or C and D) out of service would require entry into Technical Specification 3.0.3, while the proposed AOT would allow 72 hours. Again, an ICCDP and ICLERP must be calculated for these combinations. Finally, following the required basis change, two SW pumps powered from the same electrical train (i.e., pumps A and C, or B and D) could be out of service for 72 hours, since only one train is inoperable. Since the proposed AOT would allow 72 hours, there is no change for this combination, and therefore ICCDP and ICLERP need not be calculated. However, to ensure no undue risk results from this configuration, the ICCDP and ICLERP

have been calculated and included in this analysis.

The GPSA Revision 6.2 model is used for this evaluation. Ginna Station will implement an extended power uprate (EPU) during the fall 2006 refueling outage. The Revision 6.2 model reflects the post-EPU condition of the plant. The results of the ICCDP evaluation are summarized in Table 4. The table shows the ICCDP resulting from the CRFC flashing issue for each individual SW pump out of service for the proposed limit of 14 days. The table then shows the ICCDP for each combination of two SW pumps out of service for the proposed limit of 72 hours.

Table 4
ICCDP

SW Pump OOS	**Single Pump Impacts**
	14 days
A	**3.751E-09**
B	**3.717E-09**
C	**3.751E-09**
D	**3.717E-09**
SW pumps OOS	**Two Pump Impacts**
	72 hours
A & B	**3.214E-09**
A & C	2.213E-09
A & D	3.208E-09
B & C	3.208E-09
B & D	2.207E-09
C & D	**3.214E-09**

As shown in the table, the ICCDP for all possible combinations is less than 1E-08/yr, which is well below the RG 1.177 criteria of 5.0E-07. No specific ICLERP evaluation was performed since even if 100% of the ICCDP went to ICLERP, all cases would be at least a factor of 10 below the RG 1.177 criteria. In reality, it is not expected that any significant portion of the ICCDP due to the CRFC flashing issue would lead directly to an early release. This is due to the fact that the failure mechanism is a gradual heat-up of containment after sump recirculation has been initiated, which eventually leads to over pressurization of

containment and failure of emergency core cooling system (ECCS) injection due to loss of NPSH to the residual heat removal (RHR) pumps. This is a relatively slow process which would take several hours, allowing for evacuation of the emergency planning zone. Additionally, no credit has been taken for procedural guidance which directs operators to re-initiate containment spray in recirculation mode if containment pressure exceeds 28 psig. Successful re-initiation of at least one containment spray pump would drastically reduce the likelihood of containment failure and a large release, even if core damage did occur. Given that the overall GPSA LERF is approximately an order of magnitude below the CDF, a detailed calculation of ICLERP would be expected to produce a similar result.

1.1.4 Risk Insights

SW pump Importance

With a single SW pump out of service, the remaining SW pumps take on only slightly higher risk significance than normal. This is due to the fact the failure of a second pump would be required, with no recovery of either the out of service pump or the failed pump within 72 hours, or two additional pumps would be required to fail with no recovery of any of the three pumps within three hours (see Section 1.1.7 item 4 below for discussion of non-recovery probabilities). With two pumps out of service, the importance of the remaining operable SW pumps increases, since any single pump failure will result in only one operable SW pump.

DG Importance

For a single SW pump out of service, or two SW pumps from the same electrical train out of service, the emergency diesel generator (DG) on the opposite electrical train becomes risk significant. This is due to the fact that two of the three remaining operable SW pumps are powered from that electrical train. A LOCA initiating event causes a reactor trip coincident with a safety injection (SI) signal, which trips the main generator while at the same time loading the large SI loads onto the offsite power system. As a result, there is an increased potential for grid failure. Two of the remaining operable SW pumps are then relying on the DG for that train to supply power, and loss of the DG will result in one or no operable SW pumps. For two SW pumps on opposite electrical trains out of service, both DGs become significant risk contributors since failure of either will result in only a single operable SW pump.

1.1.5 Scope of PSA

The GPSA is an at-power, internal and external events PSA. Both Level 1 and Level 2 are addressed. The external events considered are fire and external flooding.

1.1.5.1 At-Power Model Structure

The GPSA utilizes the standard small event tree / large linked fault tree Level 1 methodology. Event trees are developed for each unique class of identified internal initiating events, and top logic is developed to link these functional failures to system-level failure criteria using the Computer Aided Fault Tree Analysis (CAFTA) code. Fault trees comprised

of component and human failure events are developed for each of the systems identified in the top logic with the exception of the Main Feedwater (MFW) System and the Reactor Trip System (RTS); these two systems are modeled using simplified Boolean expressions. Fault trees were also developed for systems required to support those systems identified in the top logic (e.g., electric power). Initiating event frequencies are developed, and fault tree hardware-related events are quantified with a mixture of generic data from throughout the nuclear industry and Ginna Station specific data. Solution of the model top logic yields "cutsets," or those combinations of events which lead to core damage or large early release. Fire and flooding initiating events are included in the fault tree at the appropriate locations so that the impact of the fire/flood on plant equipment and operator actions is accounted for.

1.1.5.2 Shutdown Risk Assessment

As discussed in Section 1.1.1.1 above, this change should have no impact on shutdown risk since all planned SW pump maintenance is currently done while the plant is on-line, and it is anticipated that it will continue to be done on-line.

1.1.6 PSA Detail Needed for Change

The GPSA explicitly models the functions associated with the four SW pumps and the CRFCs. Key modeling features are discussed below.

1.1.6.1 Key Initiating Events

LOCA Initiating Event Frequencies

The GPSA models loss of coolant accidents (LOCAs) based on equivalent diameter of the break. The model includes pipe break initiated LOCAs as well as transient induced LOCAs. The pipe break LOCAs are broken down by a range of equivalent diameters, and an initiating event frequency is developed for each range of break sizes, using the data from NUREG-1829. The pipe break LOCA initiating events and corresponding frequencies are:

LIS1LOCA	LOCA 0.055 inches to less than 1 inch diameter	7.89E-03/yr
LIS2LOCA	LOCA 1 inch to less than 2 inches diameter	1.49E-03/yr
LIM4LOCA	LOCA 2 inches to less than 4 inches diameter	2.32E-04/yr
LIM6LOCA	LOCA 4 inches to less than 6 inches diameter	1.08E-05/yr
LILLOCA	LOCA 6 inches and higher inches diameter	4.85E-06/yr

The transient induced LOCAs include reactor coolant pump (RCP) seal LOCAs, a single stuck open power operated relief valve (PORV) or pressurizer safety valve, and combinations of two stuck open PORVs and/or safety valves. There are three potential RCP seal LOCA sizes, all of which are equivalent to a break size of less than two inches. A single stuck open PORV or safety valve is also equivalent to a break size of less than two inches. Two stuck open PORVs and/or safety valves is equivalent to a break size of between two and six inches. The frequency of these events is calculated within the fault tree model by combining the

initiating events which result in single or multiple PORV and/or safety valve lifts with the probability that the valves fail to re-close.

1.1.6.2 Fault Tree Modeling

Failure of CRFCs due to Service Water Flashing

The GPSA fault tree for post-EPU conditions used for this analysis contains logic which addresses the failure of containment heat removal due to the service water flashing issue. For any LOCA (either pipe break or transient initiated) event with an equivalent break size of two inches diameter or greater, core damage will occur given failure of three or more SW pumps.

Loss of all Service Water Initiating Event

The GPSA fault tree contains logic to model a required reactor trip due to a loss of all service water, as well as a Technical Specification required plant shutdown due to a partial loss of service water. The current model logic is based on the current Technical Specification AOTs and therefore was modified to match the proposed, more limiting, AOTs.

Operator Actions

There are no operator actions included in the fault tree that are directly associated with the loss of containment heat removal due to the service water flashing issue. Although there are operator actions which could potentially mitigate this event (e.g., starting of a containment spray pump in recirculation mode or isolating service water flow to the non-operating CRFCs), they have not been included in the model due to the lack of detailed modeling of the impacts that these events would have. Operator actions to isolate a stuck open PORV and to start an available SW pump (given that it has not received an auto-start signal) are included in the model.

1.1.6.3 System Models

Service Water to CRFCs

The fault tree logic for failure of the service water supply to the CRFCs is modeled as all combinations of three pumps failing due to pump start or run failures, discharge check valves failing to open, or failure of the suction supply. Failures may also be due to support system failures, including 480 VAC power and 125 VDC power. There are no pump or room cooling dependencies for the SW pumps. Due to the fact that only two of the four SW pumps can be in the standby mode (i.e., receive a start signal after power has been restored to the 480 VAC bus following a loss of power) there will always be two pumps which do not receive a start signal. Thus, there may be a pump which can be manually started by the operators. The fault tree model includes this operator action. Common cause failures between like system components (SW pumps, discharge check valves, etc.) are included in the model.

1.1.6.4 Truncation Limits

The GPSA model was solved with a truncation limit of 1.0E-11. For the limiting case of a single SW pump (pump A) out of service for 14 days, a simple truncation analysis was performed by truncating the cutset file at 1.0E-09 and 1.0E-10. The results are as follows:

Table 5
Truncation Results

Truncation limit	CDF increase	Percentage of 1.0E-11 CDF increase	Increase From the Previous Decade
1.0E-09	3.026E-09	80.7%	
1.0E-10	3.476E-09	92.7%	12.0 %
1.0E-11	3.751E-09	100%	7.3 %

Although this is not a rigorous demonstration of convergence, it does provide a high degree of confidence that lowering the truncation limit would not increase the values enough to contradict the conclusion that the risk increase associated with the proposed AOT extension is acceptably small.

1.1.7 PSA Key Inputs and Assumptions

There are several key inputs and assumptions used in this analysis. These are described below.

1.1.7.1 Planned unavailability of a SW pump and the DG on the opposite electrical train is assumed to be mutually exclusive.

As discussed above, the analysis is performed with one or two SW pumps out of service and the remaining equipment at nominal expected unavailabilities. The nominal expected unavailability for the opposite train DG is based on both planned and unplanned out of service time. However, the Technical Specification for one DG out of service (LCO 3.8.1, Action Statement B.2) requires that if one DG is inoperable, the required feature(s) supported by the inoperable DG must be declared inoperable when its required redundant feature(s) is inoperable, within four hours. In this case, if a SW pump was already inoperable, the opposite train DG would not be removed from service for planned maintenance since it would require declaring the two SW pumps for that train inoperable within four hours: this would force the plant to shut down per Technical Specification 3.0.3 due to three SW pumps inoperable. Similarly, if a DG is out of service, a SW pump on the opposite train would not be taken out of service for planned maintenance. A conservative approach to modeling this is taken by determining the amount of the SW pump unavailability due to unplanned maintenance as a percentage of the total unavailability based on historical data. An average value of 44.7% was generated for the four pumps. This value was then applied as an adjustment factor to cutsets containing events for both a SW pump and the opposite train DG out of service for maintenance. The model then essentially only includes cases where a DG

is out of service for planned or unplanned maintenance and a running SW pump fails to run (i.e., becomes out of service for unplanned maintenance).

1.1.7.2 Flashing of SW downstream of CRFCs is not a concern for LOCA sizes below 2 inches.

This risk analysis addresses the increased risk due to the fact that post-EPU, a single SW pump is not considered capable of providing adequate flow to the CRFCs during sump recirculation following a design basis LOCA with a loss of offsite power and a single active failure, due to the potential for flashing of the service water in the outlet piping downstream of the operating CRFCs, which could prevent flow through the coolers. However, analysis indicates that for LOCA equivalent break sizes less than two inches in diameter, the flashing issue would not be a concern due to lower containment temperatures and later initiation of sump recirculation: therefore, a single SW pump would be adequate. As such, this issue was only included in the model for LOCA sizes of two inches in diameter and greater.

1.1.7.3 Percentage of controlled plant shutdowns result in lifting of both PORVs

The GPSA assumes that the loss of all service water initiator is equivalent to a loss of main feedwater (MFW) initiator, since SW is required to cool the MFW pumps. As such, the loss of all SW initiator is assumed to cause a lifting of both PORVs. This creates the possibility of one or more stuck open PORVs and a transient induced LOCA. However, for the cases where a plant shutdown is required by Technical Specifications due to a partial loss of service water, this is overly conservative. In cases where three SW pumps are out of service, an immediate shutdown would be required by Technical Specification 3.0.3. During this shutdown, no challenge to the PORV would be expected. However, it is possible that with only one operating SW pump, MFW could fail prior to the shutdown due to loss of cooling resulting in a reactor trip with a challenge to the PORVs. For this analysis, it is assumed that 67% of the year service water inlet temperatures are cold enough that failure of MFW due to loss of cooling is not considered likely. This is based on one incident on June 10, 2005 where the plant operated for approximately two hours with one service water pump and no failures of MFW. The SW inlet temperature at the time was approximately 62 degrees. Plant data indicates that SW inlet temperature is generally below 60 degrees from the beginning of October through early June. During the remainder of the year, it is conservatively assumed that these scenarios result in the loss of MFW. In cases where two SW pumps are out of service and are not recovered within 72 hours, two SW pumps would be available, and no failure of MFW would be expected, regardless of SW inlet temperature. However, to address the potential for operator errors or plant failures during the controlled shutdown which would cause a challenge to the PORVs, it is assumed that 10% of these controlled plant shutdowns will challenge the PORVs.

1.1.7.4 Probability of failing to recover failed SW pumps prior to required shutdown.

Under the proposed Technical Specification, with a single SW pump out of service, the failure of a second pump would require entry into a 72 hour LCO following which a plant shutdown would be required. However, if either pump is recovered prior to the 72 hours, no shutdown is required. Therefore, an assumption is made that there is a 10% probability that neither pump is recovered prior to the expiration of the 72 hour limit. This is considered

reasonable since only one pump needs to be restored. It is expected that repair efforts would continue around the clock to prevent a shutdown and only the most catastrophic failures of the pump or motor would be expected to require longer than three days to fix. Similarly, if a single SW pump is out of service and two more SW pumps fail, or if two SW pumps are out of service and a third fails, LCO 3.0.3 would be entered immediately. For this case, an assumption has been made that if any of the three out of service pumps is restored within three hours (half the time to be in Mode 3) the plant would return to full power with no shutdown. The non-recovery probability for these scenarios has been assumed to be 0.5. This is also considered reasonable given that many failures can be corrected in a short time frame. As discussed in Section 1.1.9, below, the results of this risk analysis are only very slightly sensitive to the values used for these non-recovery probabilities.

1.1.9 PSA Sensitivity/Uncertainty Analysis

To evaluate the sensitivity of the SW pump required action completion time to variations of key contributing parameters, a series of sensitivity cases were evaluated. The sensitivity evaluation is based on a doubling of the following key parameters:

- LOCA frequencies
- Failure likelihood of operators isolating one or more stuck open PORVs
- SW pump non-recovery probabilities assumed

The first two parameters are considered key based on cutset examination, while the third addresses assumptions which are made in the model without a detailed technical basis. Based on the results of the sensitivity studies, there is a high degree of confidence that the proposed SW required action completion time extension results in an acceptably small risk increase.

1.1.9.1 LOCA frequencies

A review of the cutset results for the most limiting case (SW pump A or C out of service for 14 days) indicates that pipe break LOCA initiators contribute 67.1% of the total CDF increase of 3.751E-09/yr. Thus, doubling these initiating event frequencies would result in a further CDF increase of 3.751E-09/yr * 0.671 = 2.517E-09, or a total CDF increase or 6.268E-09.

1.1.9.2 Failure likelihood of operators isolating one or more stuck open PORVs

One of the most significant operator actions related to this analysis is the need for operators to isolate a stuck open PORV to mitigate a transient induced LOCA. This failure event contributes 31.2% of the total CDF increase of 3.751E-09/yr for the limiting case of SW pump A or C out of service for 14 days. Thus, doubling this operator action failure likelihood would result in a further CDF increase of 3.751E-09/yr * 0.312 = 1.170E-09, or a total CDF increase or 4.921E-09.

1.1.9.3 Non-recovery probabilities for failed/OOS SW pumps prior to required shutdown

As discussed in section 1.1.7.4, above, assumptions have been made as to the likelihood that out of service or failed SW pumps will be recovered prior to having to having to shut down the plant due to the Technical Specification LCO requirements. These failure events contribute 0.125% of the total CDF increase of 3.751E-09/yr for the limiting case of SW pump A or C out of service for 14 days. Thus, doubling this operator action failure likelihood would result in a further CDF increase of 3.751E-09/yr * 0.00125 = 4.689E-12/yr, or a total CDF increase or 3.756E-09/yr. Note that for the case of two SW pumps out of service for 72 hours, these events contribute 15.8% of the total CDF increase of 3.208E-09/yr, such that doubling the failure likelihood would result in an increase of 5.069E-10/yr, which is larger than the single pump case. However, the total CDF increase of 3.715E-09/yr is less than the above case.

1.1.10 Quality of the Ginna PSA

The Ginna Station Level 1 and Level 2 PSA Model was initially developed in response to NRC Generic Letter 88-20 (Individual Plant Examination, or IPE). Since the original IPE submittal, the PSA has undergone several model revisions to incorporate improvements and maintain consistency with the as-built, as-operated plant.

The GPSA Revision 5.0 update involved extensive revision of the human reliability analysis, along with enhancements to thermo hydraulic analysis, fire modeling, station blackout modeling, and steam generator tube rupture modeling. In addition, the RCP seal LOCA modeling was revised to current Westinghouse standards (Westinghouse Electric Company WCAP-16141, *RCP Seal Leakage PRA Model Implementation Guidelines for Westinghouse PWRs*, August 2003.). Overall, the GPSA was reviewed and upgraded with a goal of increased fidelity. Since that time, GPSA Revision 5.2 has been generated, which includes additional upgrades to the model, including use of higher loss of grid frequencies as recommended in "Station Blackout Risk Evaluation for Nuclear Power Plants" (NUREG/CR-INEEL/Ext-04-02525).

The GPSA Revision 6.x model series parallels the Revision 5.x development, however, Revision 6.x addresses the post-EPU plant configuration. A discussion of the EPU modeling can be found in the Ginna EPU submittal.

Overall, the GPSA is a living document that is updated and maintained to adequately reflect the as-built, as-operated plant. A procedurally controlled change impact evaluation process (Ginna procedure EP-3-P-0306) ensures that changes to the plant are reviewed for impact on the PSA. This process is integrated with the Ginna Plant Change Process, Equivalency Evaluation Process, and Setpoint Change Process such that the originator of the change and a PSA engineer determine if the change impacts the PSA. In addition, the procedure change process requires that any change, addition, or deletion of operator actions, or change to step sequence, in the Ginna Emergency/Abnormal Operating Procedures is reviewed for impact on the PSA (Ginna procedure A-601.6).

1.1.10.1 Model Peer Review

In May 2002, the Westinghouse Owners Group performed a Peer Review of the GPSA Revision 4.1. The peer review final report was issued in December, 2002 (*R. E. Ginna Station PSA Peer Review Report*, Westinghouse Electric Co., December 2002; *PSA Peer Review Certification Process Guidance*, SAE/RRA/101(98)-A, Westinghouse Energy Systems, 1998). The GPSA received a grade of full 3 for one of the technical elements, and a grade of 3 with contingencies for all other technical elements. The contingencies were due to outstanding facts and observations (F&O's) identified during the peer review. Since the completion of the review, the majority of the peer review F&O's (all six A-level and thirty three of thirty five B-level) have been addressed. A list of all A and B level F&O's, and their resolution, is provided below. The two remaining peer review comments that are not fully addressed (F&O's AS-13 and DE-01) are evaluated to ensure that they do not effect the ability of the model to estimate the risk impact of the proposed change, as discussed in the resolution of each of these items.

The following is a list of Level A and B observations and resolutions. The model revision in which the observation was resolved is shown at the end of the resolution:

- *INITIATING EVENTS IE-01 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The LOSP is divided into two parts- loss of the grid and loss of the switchyard. The grid loss includes severe weather and grid disturbances. The process of derivation of grid loss frequency uses generic NSAC data and removes any weather or grid related failure that is not applicable to the Ginna site. But no operating time is removed from the denominator.

The mean value of the generic prior for grid loss is 7.8E-3 with an error factor of 15. When Bayesian updated with the site specific data of zero failures in 14 years, the result is 2.63E-3.

Ginna uses a moment matching Bayesian update code which can produce non-conservative results, particularly when updating with zero failures. The final value of 2.63E-3 is not supported by the generic data or the plant specific data. The low value of 2.63E-3 results from the use of the specific Bayesian update combined with the selection of the error factor. If the EF of the prior is changed to 5, the result is in the range of 7E-3.

There are 3 observations:

1) the elimination of events not specific to Ginna is not appropriate for development of a prior, unless the operating hours of the (non-applicable) plants is also reduced.

2) the choice of an error factor of 15 for the prior biases the posterior.

3) the use of a moment matching Bayesian update code yields answers that can not be supported by the existing data. (Also see related F&O IE-07)

Resolution: The current PSA analysis includes all severe weather phenomena, whether or

not feasible at the Ginna site, in the LOOP calculation and uses a non-moment matching Bayesian update process. Revision: 4.2

- *INITIATING EVENTS IE-03 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The initiating event with the highest contribution to CDF in the internal events model is loss of service water (TI0000SW). The dominant contributors to this initiator are commonalties related to the intake and/or screenhouse (SWCXXSUCTI), and failures of the traveling screens. The frequency for event SWCXXXSUCTI is based on engineering judgment. The basis for this frequency is presented in Section 3.4.2.8, in the form of a review of historical records/events related to SW intake. These events provide a good starting point for a quantitative assessment, but as one of the top scenarios contributing to CDF from internal events, the analysis should be strengthened.

The fault tree logic used to quantify the traveling screen failure contribution to TI0000SW should also be revised. The current model combines the independent failure of three traveling screens with the fraction of time the screens are needed. This fraction is, with no documented basis, assumed to be 1.0E-3, equivalent to about 8 hours per year. Also, a common mode failure should be modeled for the failure of the three screens. The failure rates used for the screens in the PSA is based on all periods of operation. The use of the 1.0E-03 fraction in combination with the failure rate requires that the failure rate be developed under the condition of high stress. Therefore, the current failure rate may not applicable during the 8 hours during the year when the screens are assumed to be needed.

Resolution: Enhanced the PSA analysis for common cause failure (CCF) of the service water (SW) pumps and loss of all SW due to loss of the intake structure for the loss of SW initiator. In addition, the PSA final report has been enhanced to provide further discussion. Revision: 4.2 and 5.0

- *INITIATING EVENTS IE-04 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The partial loss of feedwater initiating event was subsumed and quantified as a reactor trip in the GPSA model. This is non-conservative since the model reactor trip model takes credit for recovery of main feedwater.

Resolution: New logic has been added to include specific initiating events for events where one train of MFW is lost and is unrecoverable. Revision: 4.3

- *INITIATING EVENTS IE-05 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The calculation of CCF basic events for support system initiators (i.e., loss of air, total loss of service water, loss of CCW) has some problems. The CCF events appear in the fault trees and utilize Alpha factors from NUREG/CR-5497, but the exposure times associated with the events are set to values less than 8760. For example the global CCF event for service water failure has an exposure time of 72 hours. In the CCW initiating event tree, CCF of both CCW pumps to run is "anded" with failure of the standby pump to start. This is a non-minimal cutset, as the CCF event alone fails both pump trains.

This miss-use of CCF events has been identified in several plant PRA peer reviews. The problem stems from the fact that when the CCF parameters from the NUREG are applied over a 8760 "mission time", the resultant system failure frequency is much, much higher than what is suggested by industry data (e.g., zero loss of CCW events in more than 2500 years of commercial operation.) But reducing the mission time for the CCF events is not an appropriate solution.

Resolution: Re-analyzed CCFs for loss of Service Water, Instrument Air/Service Air and CCW initiators. Revision: 4.2

- *INITIATING EVENTS IE-07 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The Bayesian update process for some initiating event frequencies used a moment matching technique (transformation of form lognormal to Gamma back to lognormal). This technique can cause an underestimation of the resultant frequency when the plant specific data indicates zero failures, which is the case for a number of initiators. For example, the updated GPSA frequency for grid related loss of offsite power is 2.63E-3. A more rigorous Bayesian update, without moment matching yields a result of 4.46E-3.

Resolution: Employed a non moment matching Bayesian update process to calculate initiator frequencies for Ginna Station. Revision: 4.2

- *ACCIDENT SEQUENCE EVALUATION AS-01 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: Several items were noted in review of the ATWS sequence logic in the CDF fault tree:

(1) In the ATWS fault tree logic, under Gate TL_LT (failure of long-term reactivity control), under the mechanical rod insertion failure logic, operator failure to implement emergency boration is "AND"ed with operator failure to trip rod drive MG sets (probability 1E-2). But if the rods did not insert as a result of mechanical faults, then the operator action to trip the MG sets could not be effective, and so this action should not be factored into the cutsets here. So the value of the cutsets at TL_LT should be of the order 1E-2 rather than 1E-04 as in the current model.

(2) In the ATWS fault tree, under Gate TL_KE1 (Electrical failure of RTS), failure of both reactor trip breakers is included under an AND gate, which is the common cause failure of the reactor trip breakers. Individual breaker failures are not explicitly modeled; instead, a module (Gate TLCCFBRKRF) is used to represent the effective common cause contribution of breakers RCCBV52RTA and RCCBV52RTB. That is, the failure probabilities entered for the two independent events is the square root of the assigned common cause failure probability. The common cause value assigned is the 5% lower bound value from NUREG/CR-5500 (4.6E-08), but this appears to be an optimistic interpretation of the NUREG values, with no explanation provided. Since Reactor Trip breaker failure contribution typically dominates electrical failure contribution in other models due to

common cause, additional justification should be provided as to why it is insignificant (order of E-08) in this model.

(3) In the ATWS fault tree, under Gate TL_ATWS11, there are several sequences which involve electrical failure of the RTS (as in Gate TL_KE1 noted above) ANDed with other failures and also OPERATORS FAIL TO MANUALLY INSERT RODS OR TRIP MG SETS. But the logic under Gate TL_KE1 includes Operators Fail to Trip Rod Drive MG Sets During ATWS, and the two actions, which appear to be closely related, if not identical, have different basic event identifiers. Thus, the cutsets under Gate TL_ATWS11 credit 1E-04 from operator actions, whereas it appears that a strong dependency between the two actions should be accounted for. (Ginna PSA personnel indicated that these actions had passed the HEP=1.0 screening evaluation, i.e., they had not shown up in cutsets above the truncation when their probabilities were set to 0.1.)

Resolution: The required logic changes have been made to the ATWS portion of the model. Revision: 4.2

- *ACCIDENT SEQUENCE EVALUATION AS-07 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The PSA includes credit for many recovery actions that are performed outside the control room. Accident sequence dependencies such as adverse environment, lack of access, lighting, room cooling, and availability of special tools are not explicitly addressed. As examples, operator actions AFHFDALTTD, AXHFDCITYW, and DGHFDCITYW do not discuss the performance shaping factors associated with performing local actions.

Resolution: Loss of lighting for all operator actions was incorporated in the model. Updated HRA calculations were performed using the EPRI HRA Calculator, which includes performance shaping factors for ex-control room actions. Revision: 4.3 and 5.0

- *ACCIDENT SEQUENCE EVALUATION AS-08 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The RCP seal LOCA model is appropriate. However, according to the write-up in Section 4.2.2.3.2, a 480-gpm/pump leak will result in a LOCA that is equivalent to a 1.08" break. Small-small LOCAs are considered to be < 1", and small-break LOCAs are considered to be 1" - 2". According to this definition, RCP seal LOCAs should be treated as small LOCAs, whereas transfer is made to the small-small LOCA event tree during loss of RCP seal cooling events.

Resolution: The justification for including these LOCAs in the small-small category was developed and added to Section 4.2.2.3.3 of the Final Report. Revision: 5.0

- *ACCIDENT SEQUENCE EVALUATION AS-10 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The following observations were made on the logic of event tree TL, for sequences after failure of event SG.

Event SG questions a faulted steam generator, due to several causes. Event MS asks for isolation of both steam generators in response to the faulted steam generator. Event B1 asks for steam generator cooling from 1 of 2 steam generators. Heat removal is not possible through the faulted steam generator. The fault tree logic of B1 is not sufficient to match the failures in MS and SG to prevent feeding of the faulted steam generator. Ergo, the event tree allows feeding of the faulted steam generator.

This can have an impact on LERF that is not presently included in the model.

Resolution: The fault tree model was updated to correctly address use of faulted/non-faulted steam generator. Revision: 4.2

- *ACCIDENT SEQUENCE EVALUATION AS-11 LEVEL OF SIGNIFICANCE: A*

Peer Review Observation: The following observations are on the SGTR event tree and top logic:

1) The success criteria in event B1 and L1 are 1/2 SG. Thus, the ruptured steam generator can be used for heat removal. If the ruptured SG is used for heat removal, the end state of the sequences must be cold shutdown, rather than hot shutdown. The end state for success of B1 is hot shutdown.

2) Event I2 asks for closure of the ruptured SG ARV. However, there are sequences where the ruptured SG is used for heat removal. So closure of the ARV is not possible. The logic is not sufficient to capture these as failed states.

3) Event I1 asks for isolation of the ruptured SG. Failure then goes to B1, which allows heat removal with the ruptured SG. Nowhere on this path is event UH2 asked for.

This event tree is not sufficiently detailed to track the faulted and/or ruptured status of the SGs, which is needed to develop probabilities for core melt induced tube rupture.

Resolution: Fault tree model was reviewed and revised to distinguish heat removal in the intact versus ruptured and faulted steam generators. Revision: 4.2

- *ACCIDENT SEQUENCE EVALUATION AS-13 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The Ginna PSA model is a comprehensive model, which includes fire, floods, shutdown, spent fuel pool and fuel handling accidents. All these accidents are included in the same top logic fault tree. The tree is very complex (rightfully so). The tree not only includes all these initiator types, but there are many special phenomena which only pertain to a certain mode, or certain type of event. The tree makes use of AND gates and FLAGS to associate certain phenomena with certain reactor conditions.

The tree is probably difficult to print out. No print out was available for the review. The tree is difficult to review. During the review, the team found 3 (possibly 4) AND gates which

should have been OR gates. This is disturbing given the short amount of time afforded to review the tree and the unfamiliarity of the reviewers with the model.

The review team believes that it is likely that there are additional mistakes in the logic structure. It is recommended that steps be taken to simply the tree for review and quality check and that a systematic review of all logic structure be performed.

Resolution: Significant reviews of the model logic and corrections of any errors have been made as a part of developing revisions 4.2, 4.3, and 5.0. In addition, the model is used on a daily basis as part of the 50.65(a)(4) program for the site. For issues associated with the SW AOT extension, corresponding parts of fault tree logic development have been checked for correctness. Additionally, cutset results have been evaluated to ensure expected cutsets are present and that cutsets make sense. Based on prior model reviews, and reviews specifically associated with this submittal, model fidelity has been assured for use in the risk evaluation of the SW AOT extension. Revision: 5.0

Note: The spent fuel pool model is for information only. The spent fuel pool does not contribute to CDF and is not considered in the SW AOT extension risk evaluation.

- *THERMAL HYDRAULIC ANALYSIS TH-02 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The SGTR event tree branches to the SBO event tree if station blackout conditions exist. In the SBO tree, top logic for HRX questions the probability of power recovery at "X" hours. For SGTR, this top event is defined as power recovery at 5 hours, based on information in Appendix B.3 of the PSA report. Appendix B.3 states that, based on MAAP run RUH2J, the time to steam generator dryout " ... following a SGTR (0.664 inch LOCA) with only one AFW pump available, ...the SG dries out at 4 hours with fuel damage at 5 hours." A check of the available information for MAAP run RUH2J (as provided in Table 4-2 of the PSA Report and in a fax of MAAP plots included in a notebook with a May 28, 1996 letter transmitting MAAP analysis results) indicates that time to TCRHOT > 1800 deg F is actually closer to 5.5 hours. But perhaps more importantly the information provided for this case indicates that credit is taken for 2 accumulators. In the SBO event tree (and the associated fault tree logic for SGTR with SBO), accumulators are not required.

There are 3 points to consider regarding the above:

(1) It is not clear that the time to core damage for the scenario modeled in the fault tree (i.e., no credit for accumulators) is applicable to the fault tree model, given the credit for accumulators. If the time to core damage were significantly shorter without accumulators, there could be a significant change in the probability for basic event ACAZDLOSP5 (currently 0.097).

(2) If point (1) were not applicable and there was no significant impact due to the credit for accumulators in the MAAP run, the time to core damage would be 5.5 hours instead of 5 hours. This is relatively important in the event/fault tree logic, because the model effectively assumes that power recovery at X hours avoids core damage. Since the supporting power

recovery calcs in Appendix B.3 and B.5 use the values at 5 hours, a supporting MAAP analysis that showed core damage at 5 hours would be invalid. But if there is actually 5.5 hours to core damage (i.e., to allow time for implementing pump startup recovery actions at the 5-hours power recovery time), then the modeling assumptions would be correct. (Note that a similar comment applies to the SBO-related SLOCA recovery X-hour value; the 2.25 hours reported is a core damage time from MAAP but is used as a power recovery time in the model).

(3) The same recovery times and probabilities are used in the RCP seal LOCA model (discussed in Appendix B.4), so the extent of the impact of the error is broader than SGTR-SBO.

Resolution: The fault tree was updated to address the need for accumulators for SGTRs and small LOCAs under SBO conditions consistent with the MAAP runs referenced in PSA Final Report Appendix B. Revision: 4.3

- *THERMAL HYDRAULIC ANALYSIS TH-03 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: This observation provides some comments on interpretation and documentation of analyses that support PSA success criteria.

A relatively large number of MAAP analyses were performed in the past for transients, SGTR, SLOCAs, etc., and high level results for all the cases are summarized in Table 4-2 of the PSA Report. It is not necessarily clear from the documentation in the table, and in the limited other available analysis results information, what the various cases are supposed to demonstrate, if they actually support a modeled success criterion, etc.

An example is for SGTR. Among the sensitivity cases run are cases RUH2F and RUH2G, which vary the value of MAAP parameter VFSEP (case 2F uses a value of 0.3, case 2G uses a value of 0.7, the value used in cases 2A through 2E is not stated but a check of an available MAAP parameter file listing for Ginna showed a value of 0.6, which is near the upper end of the MAAP User Manual range of allowable values of .01 to .65).

Per the MAAP user manual, VFSEP specifies the maximum void fraction value at which natural circulation cooling can occur; for void fractions above the specified value, phases separate, and a reflux cooling heat transfer mode is used, which is less efficient. The reported results for case 2F, with the lower VFSEP, show better cooldown whereas the results for case 2G with the higher VFSEP show core damage.

Several observations are offered:

(a) It is interesting that the MAAP analyst apparently recognized a potential sensitivity of the SGTR results to the value of VFSEP and thought to check on the appropriateness of the value used and sensitivity to other values. But apparently no documentation of the conclusions or insights reached based on the sensitivity analysis are available, and the MAAP analyst(s) are no longer with RG&E. The reviewers were aware of an EPRI document (TR-100167) that indicates that the 0.6 value used for Ginna is the recommended value, and that no sensitivity

analyses are needed.

(b) The results of the VFSEP sensitivities performed seem counter-intuitive in that as VFSEP is increased, such that presumably better heat transfer can occur longer, the results get worse. An explanation of what is going on in the analyses would help improve confidence in the results.

(c) There are several other cases (e.g., RUH2C and RUH2D) where it is not clear why the variations were run and for which the results of one case or the other (in this case 2D) are not clearly success and may be sensitive to the value of parameters such as VFSEP. In this particular instance, the "Result" for 2D says no core melt but RCS voiding. If this case were important to determining success criteria, its sensitivity to VFSEP could also be important. In addition, the available plots for these cases, for which it is stated that cooldown is via the intact SG, imply instead that cooldown is occurring via the ruptured SG.

Resolution: The original MAAP runs were confirmed or updated using PCTRAN (Ginna design analysis DA-NS-2005-038). HRA event timing that effects the SW AOT risk analysis have been confirmed or modified based on updated PCTRAN runs. Revision: 5.2

- *SYSTEM ANALYSIS SY-02 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: ES 1.3, step 5 indicates that if only one CCW pump is available (due to pump failure, lack of electric power support, etc.), then operators must isolate nonessential CCW loads and align CCW to only one RHR heat exchanger. There is a high-level operator action in the model for aligning for recirculation, and aligning CCW is part of the process of aligning for recirculation. However there is not a specific operator action for the case that a CCW pump is failed and some potential failure combinations are not being developed as cutsets. Model fidelity would be better if a specific operator action was incorporated at a lower level in the logic as an input to the specific impacted components.

Resolution: A review of this operator action indicates that the current HRA event is appropriate and no change is warranted.

- *SYSTEM ANALYSIS SY-03 LEVEL OF SIGNIFICANCE: A*

Peer Review Observation: Several fault tree gates were modeled as AND gates, when the logic implies they should be modeled as OR gates. Three examples are as follows:

a) Gate TL_D_CD
b) Gate AF686A
c) Gate AX950XZ

Resolution: The fault tree model has been updated to correct the modeling issues. Revision: 4.2

- *DATA ANALYSIS DA-01 LEVEL OF SIGNIFICANCE: A*

Peer Review Observation: The Ginna PSA uses moment matching in the Bayesian update process for developing component failure rates and initiating event frequencies. Lognormal distributions are transformed into Gamma or Beta distributions, then the update is performed, and the resultant distribution converted back to a lognormal form. This method produces good (i.e., approximately equal to more rigorous methods) posterior mean values when the plant specific data consists of a non-zero number of events. However, when the evidence consists of zero failures in "n" demands (or hours of operation) this method will consistently under-estimate the mean value of the posterior distribution. As an example, the posterior mean for "AF AV C" in Table 7-5 is listed as 1.75E-04. When this update is performed (0 failures in 884 demands) rigorously by updating the discrete lognormal probability distribution directly (using ERIN BART software), the result is 4.77E-04, nearly a factor of 3 higher than the Ginna PSA value.

Although the problem only occurs when updating with zero failures, it is noted that 184 of the 278 component failure rate updates listed in Table 7-5 involve updates with zero failures.

An additional observation regarding this method is that when updating with zero events, regardless of the number of demands, the error factor of the posterior is equal to the error factor of the prior. This is apparently another weakness of this method.

Resolution: PSA calculations now use an updated Bayesian technique which does not employ moment matching. Revision: 4.2

- *DATA ANALYSIS DA-04 LEVEL OF SIGNIFICANCE: A*

Peer Review Observation: The mean value used in the PSA for failure of the turbine driven AFW pump to start on demand was grossly under-estimated due to an error in the Bayesian update process. The wrong distribution was selected as the prior in the calculation of the subject failure rate (AF TP A).

Resolution: Used the correct prior in calculations; results included in the model. Revision: 4.2

- *DATA ANALYSIS DA-06 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The basis for RPS control rod and reactor trip breaker CCF frequencies should be revised and/or better documented. The following information is taken from Table 7-6 of the PSA report.

Control Rod - Fails to insert mechanically Rod)	2E-07 (5th %tile from NURGG/CR-5500, T3,
Control Rod - Fails to insert electrical BME)	1.6E-06 (mean from NURGG/CR-5500, T3,

Reactor Trip Breaker - Fails to open 4.6E-08 (5th %tile from NUREG/CR-5500, T3, BME)

There is no documentation regarding the use of 5th %tile values from the source as mean values in the PSA. There is no documented basis for using the 5th %tile values. It appears that the control rod CCF failure modes above should be combined and use the mean value for ROD from Table 3 of NUREG/CR-5500. The reactor trip failure mode should use the mean value listed for BME in the same table.

Resolution: The RPS/reactor trip breaker logic has been reviewed and revised. Revision: 4.2

- *HUMAN RELIABILITY ANALYSIS HR-02 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: Table 7-15 states that the screening value of 0.01 for operator action RCHFD00MRI was derived from page B-7 of WCAP-11993. However, WCAP-11993 gives the HEP for manual rod insertion (MRI) as 0.1, not 0.01.

Resolution: The correct value of 0.1 has been used for this action. Revision: 4.2

- *HUMAN RELIABILITY ANALYSIS HR-04 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: All pre-accident HEPs were quantified using screening values of 3.0E-3, consisting of 0.03 for the basic HEP times 0.1 for recovery. While no one pre-accident HEP has high risk significance, using screening values for pre-accident HEPs could have an impact on the risk assessment for maintenance configurations. While it is understood that many pre-accident HEPs may be identical due to identical processes (e.g., failure to restore a component following testing usually involves an independent verification, and failure to restore a component following maintenance involves performing a post-maintenance test), plant-specific HEPs could be derived for each type of error and applied to each type of activity.

For example, the HEP for failing to restore a component after maintenance typically includes restoring the pump suction and discharge valves. Assuming that a post-work test is performed, the HEP for such a case could be calculated as 2 x 0.03 x 0.01 x 1.6 x 1.6 = 1.5E-3, where the 1.6 factors are used to convert the median HEPs to mean values. For test restoration errors, using ASEP would result in a mean HEP of 0.03 x 0.1 x 1.6 x 1.6 = 7.7E-3, which is actually higher than the screening HEP (which uses median values).

The HEP associated with mis-calibrations would need to consider the recovery mechanisms available.

Resolution: The methodology for pre-initiator HEPs has been updated to address these issues, and the final report enhanced. Revision: 4.3

- *HUMAN RELIABILITY ANALYSIS HR-08 LEVEL OF SIGNIFICANCE: A*

Peer Review Observation: The method and process for assessing dependent human actions does not meet the objectives of the peer review guidance. The following observations were made of the current process to identify and quantify dependent human actions:

1) A systematic search was made of the quantified cutsets for dependent HEPs in the same sequence. The starting point for the search, however, was the set of cutsets quantified at a 1E-10 cutoff. Thus, many of the "untreated" HEP combinations could have been eliminated.

2) There is no analytical process for HEP adjustment for multiple HEPs in the same sequence. The adjustment process was to adjust the last HEP in the sequence to a value of 0.1.

3) This process resulted in adjustments for a limited number of HEP combinations. Several of the common HEP combinations found in other PRA's (AFW / MFW / F&B) were not represented.

4) Even with the correction factors, some of the HEP combinations found in the final cutsets had very low combined failure probabilities, e.g., 1.7E-06 (LISSLOCA), 1.6E-07 (FL00TB6), 7.6E-07 (TIIAWTS).

Some expected combinations that were not found are:

MFHFDMF100 * RCHFD01BAF * AXHFDSAFWX
MSHFDISOLR * RCHFDCDPPR * RCHFDCDTR2 * RCHFDCOOLD
AFHFDSUPPL * MFHFDMF100 * AXHFDSAFWX * RCHFD01BAF

Resolution: An enhanced approach for post-initiator HRA, which identifies dependencies a priori, not just for HEP's in dominant cutsets, was used. Additionally, for Revision 5.0 the model was quantified with all HRA events set to a value of 0.25 and all resulting combinations examined for dependency. Dependent events were then included in the model logic. Revision: 4.2 and 5.0

- *HUMAN RELIABILITY ANALYSIS HR-09 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: Event AFHFDSUPPL:

This event is discussed in the HRA notebook as if it is the refill of the CST, from other sources. The timing, and PSF seem to consider that the CST is to be refilled from hotwell or elsewhere.

However, the fault tree uses this event as input to gate AF460, which is an AND gate. The fault tree appears to consider the CST is refilled automatically from the hotwell, and this event "SUPPL" is for refill of the CST from other sources after the hotwell is depleted. If this is true, then the cues and PSFs are inappropriate.

Alternatively, gate AF460 could be an OR gate, and the PSF for this event would be correct.

Resolution: The methodology for HEP calculation and dependent HEP quantification was updated. In addition, HEP events of significance to the SW AOT extension were re-calculated using the EPRI HRA Calculator, with the exception of event ACHFDRESTORE, which uses a conservative screening value of 0.25. Revision: 4.2 and 5.0

- *HUMAN RELIABILITY ANALYSIS HR-10 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: All HEPs are quantified as if they are the only HEP in the sequence, ignoring the other actions that will require time and effort. For example, in Loss of SG cooling sequences, the process of events will be:

1) Reactor trip
2) AFW fails - MFW is attempted to restore
3) MFW fails - SAFW is attempted to align
4) SAFW fails
5) Feed and Bleed attempted.

However, the timing for actions applicable to these sequences do not consider the other actions.

RCHFD01BAF uses a compelling signal cue at 9 minutes
AXHFDSAFWX uses a compelling signal cue at 10 minutes
MFHFDMF100 uses a compelling signal cue at 10 minutes

The diagnosis errors for these HEPs are:

RCHFD01BAF = .0032
AXHFDSAFWX = .00261
MFHFDMF100 = .008

(note that these numbers imply it is more difficult to realize the need for MFW than for SAFW and F&B. In reality, MFW would be the first system for SG heat removal after AFW failed.)

A more realistic analysis would consider the compelling signal for MF to be at 9 minutes. The compelling signal for SAFW would be sometime after MFW is known to be failed and the compelling signal for Feed and bleed is when SG water level reaches the cue indicated in FRH.1 (certainly not 10 minutes).

Resolution: The methodology for HEP calculation and dependent HEP quantification was updated. In addition, HEP events of significance to the SW AOT extension were re-calculated using the EPRI HRA Calculator, with the exception of event ACHFDRESTORE, which uses a conservative screening value of 0.25. Revision: 4.2 and 5.0

- *HUMAN RELIABILITY ANALYSIS HR-12 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The diagnosis errors are calculated using either the annunciator response model or the time based crew response model. Although both these methods are used correctly, there are no criteria as to which applies in each situation. It appears that the lower probability was used when desired.

Resolution: The PSA final report was enhanced to include a discussion regarding when to use the Annunciator versus the Time Response diagnostic models in ASEP. In addition, HEP events of significance to the SW AOT extension were re-calculated using the EPRI HRA Calculator, with the exception of event ACHFDRESTORE, which uses a conservative screening value of 0.25. Revision: 4.2 and 5.0

- *HUMAN RELIABILITY ANALYSIS HR-14 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: Event RRHFDCOOLX

This event is a screening recovery of 0.1 for long term RHR sequences. There is no basis for the application or probability of the event. It is assigned as a "screening value" and therefore can seemingly be assigned anywhere without justification.

RRHFDSUCTN is also a screening value used with no apparent justification.

If both these were eliminated, internal events CDF would increase 6%.

Resolution: HEP values were calculated for these events. Revision: 4.2 and 5.0

- *HUMAN RELIABILITY ANALYSIS HR-15 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: DGHFCITYW = .0966.

This event is to align city water to the DGs in the event SW fails. The HRA analysis states the time window is 86 to 263 seconds to establish water before the DGs fail. The PRA uses 4 minutes for a diagnosis time, which is the upper bound of the time interval. In addition, if 240 seconds are used for diagnosis, this leaves only 23 seconds to align the city water.

If the true time is 86 seconds, the action cannot succeed.

If 4 minutes are allowed for diagnosis, then there is no time left for action. If 1 minute is allowed for diagnosis, the HEP is much higher.

Resolution: This event has been re-evaluated using an appropriate diagnostic time. Revision: 4.2 and 5.0

- *HUMAN RELIABILITY ANALYSIS HR-16 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: There are 3 events in the PRA that use the same HEP. They are RCHFDCDOSS, RCHFDCDTR2, RCHFDCOOLD. These are all assigned a probability of .0307. This is based on calculation of a dependent probability for a similar event (RCHFDCDOVR), which is not used any longer. These events must be conditional on the failure to prevent SG overfill during an SGTR.

The 3 events listed above appear in many sequences that do not involve SGTR or SG overfill.

Resolution: The three HEP's discussed have been re-examined for consistency and re-quantified. Revision: 4.2 and 5.0

- *DEPENDENCIES DE-01 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The specific comments below were generated during the review. Some may be resolvable by providing available documentation that the reviewers were unaware of. However Ginna PRA staff acknowledges that the level of documentation detail is limited enough that it presents a problem to analysts outside of the group. It is therefore important that additional documentation of detail be performed.

- Need documentation of impacts of initiators on the model. For example, "Flood Scenario FL00SH1 fails components X, Y, X...."

- Discussion of propagation sources were provided but were limited and hard to follow.

- Affected components must be inferred by looking at what the flood initiator is an input to in the fault tree. A listing would facilitate review – and use of the flood analysis.

- Analytical approach first defined a flood frequency for a space based on a semi-generic data set and then apportioned it according to what was felt to be important. A clear description of a systematic approach for how this was done was not found.

- Initiating event logic for service water contains gate LSW001. Beneath LSW001, the probability of air temperatures below 30 F is given as .133 and the probability of cold lake temperatures is given as .0166. They are apparently treated as independent events but it would seem that they are highly dependent. Correction or explanation as appropriate is suggested.

- Logic below gate TL_RH3Y "ands" TL_SB_F1 (fire recoveries) and FLN700 (screenhouse recoveries). This may be correct as intended but it seemed like the gate should be an "or." Correction or explanation as appropriate is suggested.

- Flood rates were not provided, but were discussed in terms of "very large, large, etc." Specific flood rates would have been helpful in the review. Also necessary to calculate operator response times. Generally sump capacities were not discussed, however for the more significant floods this does not appear to matter.

- Suggest providing a clear listing of affected SSCs.

- Need more discussion about interaction between flood frequency apportionment in Table 7-9 and additional frequency apportionment in fault tree (i.e. screenhouse flood FL000SH1 receives a "flood size apportionment" in Table 7-9 and also an additional flood size apportionment in the model).

Resolution: There are several issues discussed by this F&O. The suggested resolution of this item is to consider revising the documentation to address the issues. Two of these issues require model logic correction (bullets 5 & 6). These issues have been corrected in the model. All remaining items are solely related to documentation, and will require enhanced explanation in the final report, but have no impact on the model results. Revision: 5.0

- *DEPENDENCIES DE-02 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: Operator actions during floods should be reviewed.

• Instances were found where "normal" internal model operator recovery actions appeared in flood sequences (e.g. AXHFDCITYW), without a change in probability. This may be appropriate but the events should be reanalyzed to be sure, looking at staffing requirements, operator burden, cues, physical access issues, etc. For the example it is not obvious that the task of aligning city water would be as easy for a crew to accomplish during a flood as during a relatively normal trip which required extended AFW operation. If the detailed HRA analysis for this event under flooding conditions was provided, it would help support this model assumption.

• It is not clear that operator actions to isolate certain floods are being modeled at the appropriate level of detail in the model. For example, if a Service Water header fails in the aux building, or to the diesels, etc., it must be isolated and this isolation will impact what supported components receive service water and how. It is not clear that there are specific operator actions that address this.

• Event IFAZCIBFLI, "Intermediate building flood isolated before significant accumulation," appears to encompass an implicit operator action. No dependency assessment of this with other actions was noted.

• Aux. building floods of a certain size are assumed to be isolable by isolating valve 4734. It's not clear that the model *.fre file is correctly taking this pathway out when it should (it may be, but it wasn't obvious during review). In addition, it appears that the possibility of a flood in the parallel SW line (isolable by 4735) was not considered.

Resolution: A dependency analysis for flood and fire scenarios for HRA events has been performed and the model updated as appropriate to address bullets 1 and 3. Bullets 2 and 4 have been addressed by updating the model logic. Revision: 5.0

- *DEPENDENCIES DE-04 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: Not clear that accident sequences were redefined for use in floods, or that existing sequences which are used were reviewed to ensure applicability. This process may have been performed but it was not clear.

Resolution: This issue has been addressed by completing the dependency analysis for flood and fire scenarios. Revision: 5.0

- *STRUCTURAL RESPONSE ST-01 LEVEL OF SIGNIFICANCE: A*

Peer Review Observation: Basis for operator recovery for ISLOCA TL_LIPEN140 (failure of RHR shutdown cooling suction isolation valves and RHR suction piping) isn't clear. It would seem that failures of some suction piping sections would not be isolated by the actions proposed; some failures are apparently not isolable. Also, no modeling of sequences after a successful recovery appears to exist. If recovery is possible, there would presumably be a reactor trip with unavailability of RHR and there could even be environmental impacts on other plant systems due to the ISLOCA. This should be modeled.

Resolution: The entire ISLOCA analysis was updated. Revision: 4.2

- *QUANTIFICATION QU-05 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: At present only a parametric uncertainty analysis has been performed. Areas where additional sensitivity calculations should be performed include cases where thermal-hydraulic analyses predict only small margins for success in terms of the number of trains required or the time available for operator actions. One specific example is the impact of 1-of-2 PORVs for success in feed & bleed cooling versus 2-of-2 PORVs as contained in the actual EOPs.

Resolution: Detailed thermo hydraulic analyses have been performed for several of the GPSA success criteria, to ensure the correct success criteria are used. Further, the sensitivity evaluations discussed in Section 1.1.9, above, provides an indication that model uncertainties are not likely to affect the conclusion that proposed AOT is acceptable. Revision: 5.0

- *QUANTIFICATION QU-06 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: According to Section 8.2.1, interfacing system LOCAs (ISLOCAs) were screened at 1E-07/yr, citing GL 88-20 as justification. Given the relatively high conditional CDPs for ISLOCAs, their importance to LERF, and the cumulative impact of ISLOCA sequences which may have just fallen below the truncation value, the truncation limit should be justified. In addition, the truncation limit used should consider the impact of being in a configuration that could result in a relatively high CDF.

Resolution: The entire ISLOCA analysis was updated, including detailed calculations for ISLOCAs previously screened out as well as additional scenarios. Revision: 4.2

- *QUANTIFICATION QU-07 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: In quantification of the V-sequence frequency and any other cutsets whose frequency is proportional to X**N where X is a failure rate and N is a number of independent events in the cutset having the same failure rate, the mean frequency is not equal to the Nth power of the mean failure rate. For N=2 and the case where X is lognormally distributed,

X2 = M2 + V,

where M is the mean failure rate and V is the variance of the lognormal distribution. The problem is more complicated with N>2. When dealing with the V-sequence the failure rates are very low and the variance is very high such that the variance term dominates. When this is taken into account the Mean V-sequence frequency can easily be an order of magnitude greater than the result obtained using a mean point estimate (M2). It is not clear that this has been taken into account in the V-sequence quantification.

Resolution: Updated entire ISLOCA analysis. Revision: 4.2

- *QUANTIFICATION QU-10 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The dominant sequences show a station blackout cutset with CCF of all SWP fail to run: TIGRLOSP*SWCCFPUMPR_ALL. There is no similar cutset for CCF of all SWP fail to start. (SWCCFPUMPS_ALL). All pumps must restart after LOSP, so the additional cutset should be accounted for.

Resolution: Common cause failure of all service water pumps to start following a LOOP event has been included in the model. Revision: 4.2

- *CONTAINMENT PERFORMANCE L2-03 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: There are several event probabilities and split fractions in the LERF model whose basis is not explained. The probabilities appear to be an estimate of the analyst and are not reproducible without additional documentation. These events are:

CTAZAUXBLD - AUX Building scrubbing
CTAZEARLY2- containment failed or bypassed late
CTAZLATEFT- filtered or submerged leak path
CTAZSGSMLL-SG leaks will not lead to rapid depressurization
CTAZSGTRST-SG inventory scrubs release.

The probabilities chosen for these range from 0.01 to 0.5. The probabilities have a dramatic effect on LERF. The probabilities appear to be analyst judgment.

Resolution: Events CTAZAUXBLD, CTAZEARLY2, CTAZLATEFT, and CTAZSGTRST could not be justified and were removed from the model. CTAZSGSMLL is justified for smaller steam leaks and has been better described within the final report. Revision: 4.3

- *CONTAINMENT PERFORMANCE L2-04 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The LERF model appears to follow NUREG/CR-6595, but includes several unique features, which are not explained and not substantiated. Some of these ideas may be more advanced than the NUREG LERF model, but are not generally included in other PWR LERF models nor included in the NUREG. The purpose and basis should be explained in sufficient detail.

These items are:

1) AUX Building scrubbing of ISLOCA releases. No basis is provided to guarantee the release is through the AUX building or to establish that the HVAC system can keep up with the release if it is large.

2) scrubbing of SGTR releases.- No basis is provided to show that water will be in the SG or that the leak will be submerged.

3) fatalities from late releases- most LERF models do not discuss fatalities, but only consider LERF. No basis for the fatality split fraction was provided.

4) reduction in fatalities for early release - most LERF models do not discuss fatalities, but only consider LERF. No basis for the fatality split fraction was provided.

Resolution: The split fractions addressed here have either been removed or justified. Revision: 4.3

- *CONTAINMENT PERFORMANCE L2-05 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: Emergency Action Levels are not included in the LERF model.

Resolution: The root concern of the peer review comment was that some core damage events were not considered to be LERF even though the timing of the emergency action levels as related to release time were not explicitly evaluated. To address this, all releases that are not the result of long term containment over pressurization due to a lack of containment cooling are considered a large early release. Long term containment over pressurization due to a lack of containment cooling events will not result in containment failure until well after a general emergency. A general emergency would be declared shortly after core damage occurs. Revision: 4.3

- *CONTAINMENT PERFORMANCE L2-06 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: There are eight human interactions (HIs) that are labeled "for Level 2 only." The following things were not considered in estimating the failure probabilities for these:

(1) In a post-core damage event, the radiation in certain areas of the plant could be extremely high. No assessment of the increased stress due to high radiation has been made.

(2) Once core damage occurs, operators are directed to exit the Emergency Operating Procedures (EOPs) and enter Severe Accident Management Guidelines (SAMGs). The SAMGs are not step-by-step "cookbook" procedures like the EOPs. Neither ASEP, nor THERP, nor any other HRA method is designed for this situation.

A cursory look at the HI descriptions reveals that (with the possible exception of CTHFDLOCLX), these HIs should be begun before core damage occurs. The timing implies, however, that they could be delayed until after core damage occurs.

Resolution: The fault tree has been updated and now contains only three human actions specifically related to Level 2. Two of these actions occur prior to core damage, while the third takes place in the control room where radiation levels are not an issue. Revision: 5.0

- *MAINTENANCE & UPDATE MU-01 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: Element MU-4 identifies a list of information inputs which should be monitored to ensure that the PSA is kept up to date. It seems clear from discussions with Ginna PRA personnel that these inputs are being monitored but it is not clear that there is a formal requirement that they be monitored. Some elements are currently being tracked by virtue of the PRA supervisor's presence on various plant committees. A formal listing of the data sources to be monitored would better meet the requirements of sub-element MU-4.

Resolution: As discussed in 1.1.11 above, Ginna implemented a proceduralized process to ensure the PSA matches the as-built, as-operated plant

- *MAINTENANCE & UPDATE MU-02 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: Current PRA update procedure requires notification of "process owners," i.e. owners of programs which rely on PRA products, when a significant PRA change occurs. However the risk impact of PRA changes is apparently not evaluated unless a process owner requests it.

The intent of the peer review guidance seems to be that PRA products should be evaluated whenever the PRA is changed, whether or not this is requested. This evaluation can be at a screening level if appropriate but it should be performed and documented.

Resolution: Procedures have been revised to require generation of a tracking item to track updating of risk-informed processes, if not done at time of PSA revision release. However, this item has no impact on the quality of PSA itself.

- *MAINTENANCE & UPDATE MU-04 LEVEL OF SIGNIFICANCE: B*

Peer Review Observation: The Ginna PSA and EOOS model update procedure (EP-3-S-0710) provides a process that requires documentation of a review of each model change request. This process is executed through the use of the EOOSCRF forms.

In general, consistent documentation of a technical review process is lacking with respect to the Ginna PSA. Although many work packages (e.g., DA-MS-99-002 and others) have signoff sheets, and are signed off by a preparer and a reviewer, technical elements of the PSA documented in the PSA have no documented review. Examples include the initiating event selection and grouping, component failure methodology and quantification, system analyses including support system dependencies, operator inputs to the human reliability analysis, and others.

Based on reviewer discussions with the Ginna PSA staff, it is apparent that additional reviews have been performed for some analyses, but it is also recognized that documented technical reviews are not being done on a consistent basis.

Resolution: Ginna implemented a process to ensure the PSA matches the as-built, as-operated plant (see 1.1.11, above, for details).

1.1.10.2 Other Relevant GPSA Open Items

The GPSA configuration is procedurally controlled such that plant changes are monitored for impact on the PSA. Areas for modeling improvement are also captured. Issues requiring action are entered into the GPSA Configuration Risk Management Program (CRMP) database as a CRMP Issue. Issues are prioritized as to their potential impact on the calculated risk as follows:

A	Potential changes of five percent or more to CDF or LERF
B	Potential changes of one percent or more to CDF or LERF
C	Potential changes that enhance or have limited sequence impact
D	Documentation issues

A review of open CRMP Issues was performed to identify those that could have a potential impact on the proposed change to the SW required action completion time extension. No issues were identified.

1.2 Tier 2, Avoidance of Risk-Significant Plant Conditions

Tier 2 is an identification of potentially high-risk configurations that could exist if equipment in addition to that associated with the Technical Specification change is taken out of service concurrently, or other risk significant operational factors such as concurrent system or equipment testing are involved. The objective of Tier 2 is to ensure that appropriate restrictions are placed on dominant risk significant configurations that would be relevant to the proposed Technical Specification change.

1.2.1 Opposite Train DG

If a SW pump is out of service, the opposite train DG should not be taken out of service. Technical Specification 3.8.1, required action B.2 will prevent this from occurring.

1.2.2 Two Service Water Pumps

Having two SW pumps out of service concurrently increases overall plant risk. Per the defense-in-depth review checklist, this would create a yellow condition and require additional risk management actions. In addition, the existing quantitative on-line risk assessment process would measure the overall plant risk of the unavailability of two pumps concurrently. Refer to Tier 3, Configuration Risk Management, below. This risk is managed in accordance with paragraph (a)(4) of 10 CFR 50.65.

1.3 Tier 3, Configuration Risk Management

Tier 3 is the development of a proceduralized program, which ensures the risk impact of out-of-service equipment is appropriately evaluated prior to performing a maintenance activity. The program applies to technical specification structures, systems or components for which a risk-informed required action completion time has been granted. A viable program would be one that is able to uncover risk-significant plant equipment outage configurations in a timely manner during normal plant operation and is described in RG 1.77 as the Configuration Risk Management Program (CRMP). The need for this third tier stems from the difficulty of identifying all possible risk-significant configurations under Tier 2 that will be encountered over extended periods of plant operation.

The Ginna on-line risk assessment process helps to ensure that the decrease in plant safety for voluntary entry into a limiting condition for operation action statement is small and is acceptable for the period of the maintenance or testing activity. It also helps to ensure that the removal from service of safety systems and important non-safety equipment and the general impact of maintenance and testing is minimized. This assurance is applicable for all plant configurations and is specifically applicable to the entry into the proposed extended SW required action completion time.

Consistent with RG 1.177, the following program elements are described below:

1.3.1 On-line Risk Assessment – PRA Scope and Control
1.3.2 On-line Risk Assessment – Tools
1.3.3 On-line Risk Assessment – Process
1.3.4 On-line Risk Assessment – Level 2
1.3.5 On-line Risk Assessment – External Events

The elements of the current process are described below. Details of this process may change over time. However, the fundamentals of performing of an integrated risk assessment using probabilistic risk techniques that meets the Maintenance Rule (a)4 requirements will not.

1.3.1 On-line Risk Assessment – PSA Scope and Control

This sub-section addresses the scope and control of the PSA used to support on-line risk assessment.

1.3.1.1 PSA Scope

The GPSA used for on-line risk assessment is a Level 1 and 2, at-power, internal events and external events (fires and external flooding, only) model. The on-line risk assessment model is derived from the current revision of the GPSA. The model is modified to remove the impact of planned maintenance. In addition, the impact of the plant availability factor is removed, that is, initiating event frequencies are increased since the plant operating mode (at-power) is known. The PSA is used to assess risk in Modes 1, 2, and 3.

Lower modes of operation (Modes 4, 5, and 6) are also assessed using the GPSA shutdown model, as well as defense in depth reviews.

1.3.1.2 PSA Configuration Control

The GPSA configuration is procedurally controlled by procedure EP-3-S-0710, Changes to the Ginna Station Probabilistic Safety Assessment and EOOS Risk Monitor Models. This procedure provides the guidelines for controlling changes to the GPSA and EOOS Risk Monitor models. As stated above, a procedurally controlled change impact evaluation process (Ginna procedure EP-3-P-0306) ensures that changes to the plant are reviewed for impact on the PSA. This process is integrated with the Ginna Plant Change Process, Equivalency Evaluation Process, and Setpoint Change Process such that the originator of the change and a PSA engineer determine if the change impacts the PSA. In addition, the procedure change process requires that any change, addition, or deletion of operator actions, or change to step sequence, in the Ginna Emergency/Abnormal Operating Procedures is reviewed for impact on the PSA (Ginna procedure A-601.6). Issues requiring action are entered into the GPSA Configuration Risk Management Program (CRMP) database as a CRMP Issue. These issues are prioritized in accordance with their significance for implementation into future PSA updates.

1.3.2 On-line Risk Assessment – Tools

This sub-section describes the on-line risk assessment tools and their controls.

1.3.2.1 Description of On-line Risk Assessment Tools

The Ginna on-line risk assessment process uses the EPRI Risk and Reliability (R&R) Workstation suite of software to determine the risk configuration of the plant. These software tools include:

CAFTA suite	The CAFTA (Computer Aided Fault Tree Analysis) software is used to develop the fault tree models and supporting databases which are the basis of the GPSA as well as the EOOS Risk Monitor. CAFTA is a comprehensive suite which performs all the functions necessary to build and maintain the fault tree models.
EOOS Risk Monitor	The EOOS (Equipment Out of Service) Risk Monitor. This software application uses the GPSA fault tree models to provide risk metrics for on-line and outage risk. The risk metrics can be based on a given plant

configuration at a point in time or can be based on scheduled plant configuration over a time period

CORA	The CORA () software is used by control room operators to log equipment as unavailable. This information is then used by EOOS to develop risk metrics.

1.3.2.2 Control of On-line Risk Assessment Tools

PSA Model Input

The on-line risk assessment model used, as input into on-line risk monitor is a zero maintenance unavailability version of the base GPSA model. Control of the GPSA model is discussed in 1.3.1.2, above. The interface between EOOS and the base GPSA model is also controlled by procedure EP-3-S-0710.

Tool Software Control

The software suite used for the on-line risk assessment process has been developed by EPRI under their software control standards.

1.3.3 On-line Risk Assessment – Process

The on-line risk assessment process is controlled by Ginna procedure IP-PSH-1, Integrated Work Schedule, and IP-PSH-2, Integrated Work Schedule Risk Management. Outage risk assessment is controlled by Ginna procedure IP-OUT-1, Outage Scheduling, and IP-OUT-2, Outage Risk Management. These procedures establish the overall administrative controls, responsibilities and duties for the direction, control and oversight of risk at Ginna. The integrated risk management process uses both deterministic and probabilistic tools to identify and control risk.

1.3.3.1 Qualitative Risk Assessment

Plant personnel assess the following risks during the planning process for each planned on-line maintenance activity:

- Nuclear Safety
- Industrial Safety
- Environmental Safety
- Corporate Safety

Note: Radiological Safety is assessed through a separate process.

This risk assessment is performed using a series of checklists, contained in IP-PSH-2. Each risk area is evaluated as HIGH, MEDIUM, or LOW. Nuclear Safety HIGH and MEDIUM activities are included in the integrated probabilistic risk assessment. By including these activities, the process has an effective means of capturing potentially risk significant

activities, especially trip sensitive activities that may not have been directly in the scope of the PSA. A qualitative defense-in-depth review checklist is also used.

Outage activities are evaluated qualitatively using a defense-in-depth review checklist contained in IP-OUT-2.

1.3.3.2 Quantitative Risk Assessment

A quantitative risk assessment of each week's maintenance schedule is performed by the Integrated Work Management (IWM) group, using the EOOS risk monitor, prior to execution of the schedule. The scheduled out of service components and their out of service windows are imported into the EOOS Risk Monitor, which calculates a risk profile for the week for the core damage frequency (CDF) and large early release frequency (LERF) risk metrics. The scope of the Ginna on-line risk assessment process includes all structures, systems and components (SSCs) modeled in the plant PSA. In addition to specific components being out of service, EOOS also adjusts initiating event frequencies for certain work activities (e.g., reactor protection system channel testing increases the likelihood of the reactor trip initiator).

Each different plant configuration is then assigned risk color as follows:

Green	risk metric is < 3x baseline risk
Yellow	risk metric is > 3x baseline risk but < 10x baseline risk
Orange	risk metric is > 10x baseline risk but < 30x baseline risk
Red	risk metric is > 30x baseline risk, or absolute value of the risk metric > 1E-03/yr (>1E-04/yr for large early release)

Actions are then taken as required, per IP-PSH-2, commensurate with the risk level. If proposed plant configurations cause a risk metric to indicate a yellow condition, IWM should consider a schedule adjustment to resolve the problem and/or consider development of appropriate risk management actions.

Additionally, a limit is placed on the duration of the activity, which is inversely proportional to the actual value of the risk metric. If a risk metric or any defense in depth top level system status block indicates an orange or red condition, schedule adjustments are required. However, intentional entry into an orange condition may be allowed if approved by plant management. Entry into an orange condition is limited to twelve hours. IP-PSH-2 also details the requirements for risk management actions to be taken to reduce the risk of a planned evolution

A similar risk assessment process is used during outages, as detailed in procedure IP-OUT-2.

2.0 Performance Monitoring

The reliability and availability of the SW pumps are monitored under the Maintenance Rule Program. If the pre-established reliability or availability performance criteria are exceeded

for the SW pump trains, they are considered for 10 CFR 50.65 (a)(1) actions, requiring increased management attention and goal setting in order to restore their performance (reliability and availability) to an acceptable level. The performance criteria are risk-informed and, therefore, are a means to aid in managing the overall risk profile of the plant. The actual out-of-service time for the SW pump trains will be minimized to ensure their reliability and availability performance criteria busses are not exceeded. Additionally, as discussed above, the more limiting AOT for a single SW pump out of service will tend to reduce the actual unavailability of the pumps by requiring shorter planned maintenance outages than are currently allowed. In practice, the actual out-of-service time for the SW pump trains is minimized to ensure that the Maintenance Rule reliability and availability performance criteria for these components are not exceeded.

To ensure that the operational safety associated with the extended Technical Specification required action completion time does not degrade over time, the Maintenance Rule Program is used as discussed above to identify and correct adverse trends. Compliance with Maintenance Rule not only optimizes reliability and availability of important equipment, it also results in management of the risk when equipment is taken out-of-service for testing or maintenance.

3.0 Conclusion

Based on the above analysis, the risk increase associated with the proposed change to the SW pump AOTs is well within the RG 1.174 and 1.177 guidelines and the proposed change is therefore acceptable.

Attachment (3)

Proposed Technical Specification Changes (mark-up)

3.7 PLANT SYSTEMS

3.7.8 Service Water (SW) System

LCO 3.7.8 Four ~~Two~~ SW pumps ~~trains~~ and the SW loop header shall be OPERABLE.

APPLICABILITY: MODES 1, 2, 3, and 4.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One SW pump ~~train~~ inoperable.	A.1 Restore SW pump ~~train~~ to OPERABLE status.	~~72 hours~~ 14 days
~~B.~~ C Required Action and associated Completion Time of Condition A or B not met.	~~B.~~ C.1 Be in MODE 3. AND ~~B.~~ C.2 Be in MODE 5.	6 hours 36 hours
~~C.~~ D ~~Two~~ Three SW ~~trains~~ pumps or loop header inoperable.	~~C.~~ D.1 - NOTE - Enter applicable conditions and Required Actions of LCO 3.7.7, "CCW System," for the component cooling water heat exchanger(s) made inoperable by SW. Enter LCO 3.0.3.	 Immediately
B. Two SW pumps inoperable	B.1 Restore SW pump(s) to OPERABLE status	72 hours

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
SR 3.7.8.1	Verify screenhouse bay water level and temperature are within limits.	24 hours
SR 3.7.8.2	- NOTE - Isolation of SW flow to individual components does not render the SW loop header inoperable. Verify each SW manual, power operated, and automatic valve in the SW ~~train~~ flow path and loop header that is not locked, sealed, or otherwise secured in position, is in the correct position.	31 days
SR 3.7.8.3	Verify all SW loop header cross-tie valves are locked in the correct position.	31 days
SR 3.7.8.4	Verify each SW automatic valve in the flow path that is not locked, sealed, or otherwise secured in position, actuates to the correct position on an actual or simulated actuation signal.	24 months
SR 3.7.8.5	Verify each SW pump starts automatically on an actual or simulated actuation signal.	24 months