NUCLEAR ENERGY INSTITUTE

Anthony R. Pietrangelo
DIRECTOR, RISK AND PERFORMANCE
BASED REGULATION

January 21, 2003

Dr. William D. Beckner, Program Director
Operating Reactor Improvements Program
Division of Regulatory Improvement Programs
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: Forwarding of TSTFs

PROJECT NUMBER: 689

Dear Dr. Beckner:

Enclosed is TSTF-424, Revision 0, "Risk-Informed HPSI AOT/CT Extension (WCAP-15773)", and draft M of the industry's proposed risk management guidance for generic implementation of risk management technical specifications initiative 4B. These documents are submitted to begin the process of dialogue leading to NRC approval of the risk management technical specifications concept. This joint plant, single system submittal builds on our "Preliminary Description Paper for Initiative 4B", dated October 12, 2001. We anticipate submitting a full plant pilot for South Texas Project in the near future, which would use the same risk management guidance (as discussed below). We request that NRC reviews of the enclosures be granted a fee waiver pursuant to the provisions of 10 CFR 170.11, specifically:

1. The request is to assist in developing an NRC regulatory guide (to provide/endorse the risk management process) in accordance with 10 CFR 170.11(a)(1)(ii).

2. The request is to support NRC generic regulatory improvements (risk management technical specifications), in accordance with 10 CFR 170.11(a)(1)(iii).

We would note the following with respect to this submittal:

1. The submittal includes a CEOG topical report addressing risk impacts of various HPSI subsystem out of service conditions, assuming no other plant equipment is simultaneously out of service. This report is intended to demonstrate typical risk results in order to facilitate discussion leading to risk assessment and management guidance. The purpose is to provide an example, and it is not the intent to develop similar subsystem generic analysis for other plant systems; rather, the risk assessment and management process, when final, would provide the necessary process elements.

2. PSA technical capability for all plants implementing initiative 4B would be accomplished through the process outlined in draft regulatory guide DG-1122, or as modified in the final, approved regulatory guide. This would involve, for the internal events at power model, use of industry peer review results, along with self assessments to address the ASME PSA standard, as endorsed by NRC.

3. The attached risk management guidance would replace the existing 10 CFR 50.65(a)(4) "at power" risk assessment and management guidance for all plants implementing initiative 4B. The enhanced risk management program would continue to meet (a)(4) requirements. Due to the nature of the CEOG HPSI submittal (primary applicability to internal events at power), the guidance does not address all areas that a full plant pilot would require. In particular, external events risk assessment requirements, and shutdown risk assessment guidance would remain essentially as under current (a)(4) requirements. It is recognized that external events model requirements, assessment methods, and risk management approaches will require further development for a full plant application.

4. The attached guidance requires a quantitative assessment at power and implements risk action thresholds based on core damage frequency, incremental core damage probability (and similar treatment of large early release frequency), and accumulated risk. Different risk management action thresholds are proposed for planned versus emergent configurations. Risk management thresholds proposed herein are preliminary and would need further confirmation through pilot efforts.

5. It is recognized that risk management actions must contemplate mode changes in order to accommodate the function of technical specifications.

Figure 3.2 proposes a mode change decisionmaking process as a starting point for this discussion.

We look forward to beginning the dialogue on this important regulatory reform effort. Please contact me at (202) 739-8081 or Biff Bradley at (202) 739-8138 if you have any questions or need to meet with industry experts on these recommended changes.

Sincerely,

Anthony R. Pietrangelo

Enclosures: 1. TSTF-424, Revision 0
2. Risk Management Guidance – Draft M

c: Patricia Coates
Stewart L. Magruder, NRR/DRPM
Technical Specification Task Force

Industry/TSTF Standard Technical Specification Change Traveler

Risk-Informed HPSI AOT/CT Extension (WCAP-15773)

NUREGs Affected: ☐ 1430 ☐ 1431 ☑ 1432 ☐ 1433 ☐ 1434

Classification: 1) Technical Change Recommended for CLIIP?: Yes

Priority: 1)High

Simple or Complex Change: Complex Correction or Improvement: Improvement

Industry Contact: Bice, David (479) 858-5338 dbice@entergy.com

See attached.

Revision History

OG Revision 0 **Revision Status: Active** **Next Action: NRC**

Revision Proposed by: ANO-2

Revision Description:
Original Issue

Owners Group Review Information

Date Originated by OG: 19-Sep-02

Owners Group Comments:
(No Comments)

Owners Group Resolution: Approved Date: 04-Oct-02

TSTF Review Information

TSTF Received Date: 04-Oct-02 Date Distributed for Review: 06-Oct-02

OG Review Completed: ☑ BWOG ☑ WOG ☑ CEOG ☑ BWROG

TSTF Comments:

TSTF approved with comments on 10/28/02, TSTF approved revised draft on 11/29. TSTF approved final on 1/20/03.

TSTF Resolution: Approved Date: 20-Jan-03

NRC Review Information

NRC Received Date: 21-Jan-03

Affected Technical Specifications

Ref. 3.5.2 Bases	ECCS - Operating	
Action 3.5.2.B	ECCS - Operating	
	Change Description:	Renamed to Condition C
Action 3.5.2.B	ECCS - Operating	
	Change Description:	New Condition
Action 3.5.2.B Bases	ECCS - Operating	
	Change Description:	Renamed to Condition C
Action 3.5.2.B Bases	ECCS - Operating	
	Change Description:	New Condition
Action 3.5.2.C	ECCS - Operating	
	Change Description:	Renamed to Condition D
Action 3.5.2.C Bases	ECCS - Operating	
	Change Description:	Renamed to Condition D
Action 3.5.2.D	ECCS - Operating	
	Change Description:	Renamed to Condition E
Action 3.5.2.D Bases	ECCS - Operating	
	Change Description:	Renamed to Condition E

1.0 DESCRIPTION

This Traveler is a request to amend NUREG 1432, Revision 2, Revised Standard Technical Specifications for Combustion Engineering Plants. The proposed change provides a risk-informed alternative to the existing restoration period for the High Pressure Safety Injection (HPSI) System, allowing this period to be extended from 72 hours up to 30 days. The overall net impact of this change is considered risk neutral as the risks of continued operation are offset by implementation of contingency actions, where necessary, and by avoidance of transition risks. The proposed change is based on the attached study, WCAP-15773, "Joint Application Report for the Implementation of a Risk Management Technical Specification for the High Pressure Safety Injection (HPSI) System," (Reference 1) conducted by the Westinghouse Electric Company, LLC (WEC) on behalf of the Combustion Engineering Owners Group (CEOG).

As discussed with the NRC, the attached study describes a "proof of concept" pilot application for a single system, and as such provides a substantial level of detail. Subsequent reports by CEOG and other OGs provided to support application of this concept to other Technical Specifications will not contain this level of detail.

Because not all Combustion Engineering (CE) plants have converted to the standard technical specifications (TS) of NUREG 1432, some TSs refer to this restoration period as Allowable Outage Time (AOT) while the standard TSs denote this period as a Completion Time (CT). For the purposes of this submittal, the use of the CT acronym may be considered equivalent to the AOT of the non-standard TSs. Likewise, the Action Statements of the custom TSs will be referred to by the standard TS equivalents of Conditions or Required Actions.

2.0 PROPOSED CHANGE

The proposed change creates a new TS 3.5.2, ECCS – Operating, Condition B that includes a risk-informed alternative to shutting down the plant after the expiration of the current CT of 72 hours. Provided a risk evaluation illustrates the acceptability for continued operation given the current plant configuration, the CT may be extended for up to 30 days. Contingency actions or compensatory measures may be required to support the acceptable results of the risk assessment. The Bases associated with this specification is also proposed for revision to reflect the intent and proper use of the proposed alternative.

TS 3.5.2 allows continued power operation with an inoperable Emergency Core Cooling System (ECCS) HPSI subsystem for a maximum of 72 hours. Hence, if an ECCS train is inoperable due to preventative or corrective maintenance on a HPSI subsystem, the train must be restored within 72 hours. If this train is not restored to an operable status within this period of time, other TS requirements would direct that the plant be placed, within a specified time period, in an operating mode where alternate operability requirements for ECCS are met.

This proposal requests the addition of a risk informed Condition to TS 3.5.2 to provide actions to be taken when one HPSI subsystem is declared inoperable and the current CT (hereafter referred to as the "frontstop" CT) is not long enough to effect restoration of operability or to support preventative maintenance or modification. The outage time beyond the frontstop will be controlled via risk management processes consistent with the Maintenance Rule of 10 CFR 50.65(a)(4). A maximum CT of 30 days (hereafter referred to as the "backstop" CT) will provide a limit to the time any TS HPSI component, regardless of risk, may remain inoperable. The frontstop and backstop CTs are the constituent parts of the flexible CT approach. The

creation of a new Condition B results in the existing Conditions B, C, and D to be renamed C, D, and E respectively.

In addition to the above, existing Condition B (heretofore referred to as revised Condition C) is modified to address cases where two or more subsystems are inoperable for reasons other than Condition A or new Condition B, provided each ECCS train remains capable of supplying 100% of its assumed flow equivalent. In this event, the subsystems must be restored to operable status within 72 hours. This change is necessary since there are several events that may render a HPSI subsystem inoperable, but do not prevent the HPSI subsystem from delivering its assumed flow to the core (i.e., the subsystem remains functional). Examples of such events may include loss of HPSI pump room cooling, degradation of HPSI pump mini-recirc capability, and loss of auto-start capability of a HPSI pump.

The intent of these changes is to enhance overall plant safety by avoiding potential unscheduled plant shutdowns and the potential regulatory burden caused by the generation of Notice of Enforcement Discretions (NOED). The proposed change will integrate TS and Maintenance Rule processes to provide for increased flexibility in maintenance and surveillance scheduling.

3.0 BACKGROUND

In response to the NRC initiative to improve plant safety by assessing the risks associated with certain TS equipment related inoperabilities, the Combustion Engineering Owners Group (CEOG) in cooperation with the nuclear industry has undertaken a program for identifying features of the plant TSs that would benefit from a risk informed approach. This effort is part of an eight-tiered initiative established by the nuclear industry in 1999 (Reference 2). Several limited scope risk informed TS (RITS) improvements have already been proposed by the industry. These include an improvement to the process of treating missed TS surveillances - Technical Specification Task Force (TSTF) 358 (Reference 3), and elimination of selected mode restraints on less risk-significant components - TSTF 359 (Reference 4). This aspect of the industry RITS effort has been identified in Reference 2 as Initiative 4B. This initiative focuses on the change to selected TSs that would allow continued “at power” plant operation under conditions when the component cannot be returned to service in the defined fixed CT (frontstop) provided a risk informed assessment ensures continued plant operation results in acceptable risks. Design basis configuration control is ensured by the proposed backstop CT.

The pilot system selected for implementation of this effort is TS 3.5.2, “ECCS – Operating,” relating to HPSI System operability. This TS is selected for three reasons. First, the HPSI system is a highly risk significant ECCS mitigation system for Pressurized Water Reactors (PWR) and hence must be carefully monitored. Second, the HPSI system has numerous components reflecting multiple system functions and mitigation capabilities; thus, degraded performance or partial inoperabilities within a subsystem does not imply a complete loss of mitigation capability by the affected train. Many issues that would result in a declared inoperability of a HPSI subsystem may not be risk significant. Finally, the system has many components and valves which require periodic maintenance and surveillance. Non-risk significant degradations of HPSI subsystem components have lead to a forced shutdown (Reference 5) at one CE designed PWR and potential shutdowns at others.

The HPSI system is an integral part of the ECCS. The primary function of the HPSI system is to inject high pressure borated water into the Reactor Coolant System (RCS) following loss of inventory and reactor overcooling events. Additionally, for some CE plants, the HPSI system can be used for RCS cooling via feed and bleed emergency operations.

Variations in the HPSI system design and performance characteristics exist among CE designed PWRs. At a minimum, the CE designed PWR HPSI system consists of two (2) HPSI pumps that inject water from a borated water source into the RCS. Many CE designed PWRs include three HPSI pumps with the third pump considered to be an installed spare or "swing" pump. One or more HPSI pumps are required to be operable via the applicable TS. Borated water can be directly injected into the RCS from a Refueling Water Tank (RWT) (located outside of containment) or recirculated (following depletion of RWT inventory) from the containment building sump. Typically, the operable HPSI pumps are maintained in standby and may be actuated either manually or automatically via indications of either high containment pressure or low pressurizer pressure. Automatic actuation of ECCS components is triggered by generation of a Safety Injection Actuation Signal (SIAS).

HPSI pumps in CE designed plants have shutoff heads that range from ~1170 to 1900 psig. Use of the medium pressure HPSI pumps provides performance capability sufficient to ensure inventory makeup to the RCS following all sizes of Loss of Coolant Accidents (LOCAs) (Reference 6). Injection into the RCS is possible at several cold and hot leg locations. However, during the early phase of a LOCA, only cold leg injection is automatically initiated. Hot leg injection is manually initiated late in the larger-break LOCA sequences. Simultaneous hot and cold leg injection is required late in large LOCA sequences to prevent possible boric acid precipitation within the reactor core. Additional system design configuration information may be reviewed in the Joint Application Report (JAR) associated with this submittal (Reference 1).

Over the past several years, numerous applications have been presented to the NRC to establish risk informed CTs for a variety of systems and components. Approvals to extend the CT for an inoperable Low Pressure Safety Injection (LPSI) subsystem or an inoperable Safety Injection Tank (SIT) were obtained for many CE designed PWRs as part of a risk informed CEOG TS improvement activity.

Risk informed CT extensions were also approved separately for inoperability of one Emergency Diesel Generator (EDG), inoperability of one train of the Containment Spray System (CSS), inoperability of selected Containment Isolation Valves (CIV), and inoperability of one battery and associated battery charger (see References 7, 8, 9, and 10). These CT extensions established risk informed fixed CTs, with the intent that risk accumulation in these intervals would be controlled via a configuration control management program. These programs have been integrated into the plant's Maintenance Rule process. HPSI unavailability is tracked and reported as a performance indicator under the NRC's Reactor Oversight Process.

4.0 TECHNICAL ANALYSIS

The proposed TS change revises the existing CT requirement for the operability of the HPSI subsystems of the ECCS. Specifically, it is proposed that a new TS 3.5.2 Condition B be created to address conditions when a single inoperable HPSI subsystem cannot be returned to service within the approved frontstop CT. The current frontstop CT for a HPSI subsystem in NUREG 1432 is 72 hours.

The primary intent of the CT extension is to allow for the risk-informed processes to be used to assess the low risk conditions resulting from various maintenance activities as justification for extending the out-of-service (OOS) period beyond the frontstop CT, should a low risk

repair/activity require extended time. The proposed risk-managed TS will obviate (or significantly reduce) the need for NOEDs. This flexibility will ensure that low risk system degradations that would cause a train or subsystem to be declared inoperable can be managed and repaired/resolved in a risk informed manner.

As indicated in the risk analysis performed by WEC (Reference 1), the overall risk impact associated with a single HPSI subsystem inoperability continuing beyond the frontstop CT should be found acceptable in the majority of cases. To support this evaluation, various HPSI System component inoperabilities, possible risk significant events, and plant configurations were considered. The following provides a synopsis of the WEC evaluation. For more detailed information, refer to the WEC JAR (Reference 1).

A HPSI subsystem consists of various components, some more risk significant than others. Such components range from injection valves, pumps seals, associated piping, the HPSI pumps, and automatic or manual circuitry associated with the pumps and automatically actuated valves. Other than a loss of the pump itself, most inoperabilities do not result in a total loss of HPSI capability for the affected subsystem. In light of this fact, the overall risk associated with such an inoperability is generally very small compared to complete functional loss of an entire HPSI subsystem.

Because the loss or partial loss of a single HPSI subsystem may not pose a significant adverse impact to overall plant risk, the flexible CT is proposed for HPSI subsystem inoperabilities. In general, the risk impact associated with the specific HPSI inoperability will be assessed during the same 72-hour frontstop CT as currently exists within the TSs. When, following a risk assessment, the overall plant risk is found to be acceptable, plant operation may continue beyond the frontstop CT. Continual risk assessments, as appropriate, will be performed to ensure that acceptable risk conditions are maintained. Regardless of the low level of risk, plant operation in this condition may not exceed the proposed backstop CT of 30 days. Acceptability of risk will be consistent with the Maintenance Rule (Reference 11) in that integrated maintenance risks beyond the frontstop CT will be controlled to an incremental Core Damage Probability (CDP) of $<$ 1.0E-05. The integrated risk of the HPSI inoperability while in the extended CT will be controlled consistent with the guidance and conditions identified in RG 1.174. The methods of determining the associated risk to continued plant operation may vary among the CE fleet, dependent upon current site risk assessment capabilities. In all cases, a quantitative assessment is expected to be utilized whenever the capability exists to support this assessment type. Qualitative assessments should likewise be used where appropriate to enhance quantitative assessments or establish a risk significance when quantitative tools are unavailable.

When evaluating the integrated maintenance risk for the extended HPSI CT, the entire maintenance evolution is evaluated for simultaneous outage of other plant components. The results of this evaluation may require maintenance schedules to be altered in order to maintain a low risk significance for the extended HPSI CT. As is routinely performed at plant sites, additional evaluations are performed when unanticipated changes occur, such as the unintentional loss of another component important to safety or a change in plant operating conditions. In regard to the HPSI CT extension, such an evaluation of risk may impact the overall time in which the HPSI subsystem may remain out of service. Therefore, an additional Required Action and CT is proposed to ensure further equipment inoperabilities are evaluated against the original CT established in proposed Required Action B.2.1. A 24 hour CT is proposed for this new Required Action B.2.2.1 to perform a re-assessment of plant risk whenever other equipment becomes unavailable that may result in an increase in overall plant risk. The proposed CT provides the necessary time to re-assess risk considering the

possibility that specialized PRA staff may need to be called in to assess the change in conditions. Should it be determined that the Completion Time extension is not acceptable, Required Action B.2.2.2 provides 24 hours to either change the current plant configuration and/or establish risk management and other compensatory measures such that overall plant risk will remain acceptable for the continuation of the HPSI Completion Time extension period. This will assure risk is managed and avoid the addition of transitional risks that may occur due to other Required Actions. If overall plant risk cannot be shown to remain acceptable prior to exceeding this 24 hour period, then new Condition D must be entered, which may result in plant shutdown.

Internal and external events are also considered, either quantitatively or qualitatively, as appropriate, within the capabilities of the individual sites. As indicated in the JAR supporting this submittal, the effect of internal and external events on the risk significance of single HPSI subsystem inoperabilities is negligible. However, other component failures or planned maintenance activities simultaneous to the extended HPSI CT period may require these events to be re-assessed in the overall integrated maintenance risk evaluation.

For the various accident events described in the JAR (Reference 1), the change in the Incremental Large Early Release Frequency (ILERF) is not a significant contributor to the risk impact of HPSI inoperabilities that extend beyond the frontstop CT. Therefore, the proposed risk assessment to be performed prior to exceeding the frontstop CT may or may not include a detailed quantitative assessment of the impact on ILERF. The decision to perform an ILERF assessment is dependent on the overall plant configuration for the time period the extended CT is expected to exist (i.e., what other equipment is OOS that may have a non-negligible impact on ILERF) and should be based on sound engineering judgment. Again, the assessment of ILERF, when required to be performed, should be completed quantitatively whenever plant capabilities exist to do so.

The above discussion of how and when risk assessments are performed is an integral part of station operation in today's nuclear operating environment. The expectation of the NRC and the industry is to ensure plant risk is assessed whenever plant configuration changes important to safety occur and that such risk is controlled. Therefore, the detail associated with the regulatory guidance and station implementation of risk assessment programs is not proposed for inclusion in the TS or TS Bases change. However, the TS Bases are revised to provide a general acknowledgement of these expectations.

Once the extended portion of the CT has been entered, the cumulative incremental risk of the flexible CT will be estimated and tracked. This tracking will supplement the maintenance rule aggregate risk assessment and confirm that the annual incremental risk associated with implementation of the risk-managed TS concept is small per RG 1.174 (Reference 12).

Compensatory measures or contingency actions developed to offset the overall plant risk associated with the extended HPSI CT vary depending upon the actual HPSI component failure or maintenance activity. Examples of compensatory measures include the establishment of temporary cooling for inoperable HPSI room cooling fans or the protection of the Auxiliary or Emergency Feedwater pumps as an alternate means of core cooling for HPSI Systems that are credited as a means for once-through core cooling. Examples of contingency actions may be the development of an Operations directive to conservatively shutdown the unit upon identifying specific equipment important to safety becoming inoperable or by delaying planned maintenance currently scheduled on other equipment important to safety. Such measures are routinely practiced for all system inoperabilities that have a

significant impact on plant risk and do not present a new practice or challenge to plant operations.

In addition to the above, when two or more subsystems are inoperable except for reasons other than Conditions A or B and at least 100% of the ECCS flow equivalent to a single OPERABLE ECCS train is available, the inoperable components must be returned to OPERABLE status within 72 hours. The 72 hour Completion Time is based on an NRC study (Ref. 15) using a reliability evaluation and is a reasonable amount of time to effect many repairs. An ECCS train is inoperable if it is not capable of delivering the design flow to the RCS. The individual components are inoperable if they are not capable of performing their design function, or if supporting systems are not available. An event accompanied by a loss of offsite power and the failure of an emergency DG can disable one ECCS train until power is restored. Reference 16 describes situations in which one component, such as a shutdown cooling total flow control valve, can disable both ECCS trains. With one or more components inoperable, such that 100% of the equivalent flow to a single OPERABLE ECCS train is not available, the facility is in a condition outside the accident analyses. Therefore, LCO 3.0.3 must be immediately entered. A reliability analysis (Ref. 15) has shown that the impact with one full ECCS train inoperable is sufficiently small to justify continued operation for 72 hours. The LCO requires the OPERABILITY of a number of independent subsystems. Due to the redundancy of trains and the diversity of subsystems, the inoperability of one component in a train or subsystem does not necessarily render the ECCS incapable of performing its function. Neither does the inoperability of two different components, each in a different subsystem, necessarily result in a loss of function for the ECCS. This allows increased flexibility in plant operations when components in opposite trains are inoperable.

Reference 5 describes situations in which one component, such as a shutdown cooling total flow control valve, can disable both ECCS trains. With one or more components inoperable, such that 100% of the equivalent flow to a single OPERABLE ECCS train is not available, the facility is in a condition outside the accident analyses. Therefore, LCO 3.0.3 must be immediately entered.

The proposed less restrictive Required Actions and CTs would allow the plant to complete maintenance activities at power while avoiding a potentially greater risk associated with plant shutdown. In practice, incremental risks are managed by limiting OOS time, implementing risk important compensatory measures, periodic tracking and prospective and retrospective risk evaluations of the use of extended flexible CT. The assessment of risk takes into account both the detrimental impacts to current risk (such as other components simultaneously OOS) and the enhancements offered by compensatory measures or contingency actions. The overall impact on risk also considers the risk avoided by remaining at steady-state power operation, eliminating the shutdown transition risks that would have normally been incurred by HPSI inoperabilities that exceed the frontstop CT. These risk management factors are considered within the scope of the Maintenance Rule and are currently well established within the CE fleet. Since these factors are controlled and assessed by separate regulation, including the details of the Maintenance Rule programs with the TS or TS Bases in not necessary.

In summary, HPSI system inoperabilities are recognized as playing an important role in managing plant risks. Nevertheless, sufficient programs consistent with the guidance of the Maintenance Rule may be utilized to ensure HPSI system inoperabilities can be effectively resolved without placing the plant in an unreasonable or unnecessary risk configuration. Use of the extended HPSI CT will require the plant staff to manage the inoperability in a manner consistent with a quantitative or semi-quantitative (blended) implementation of the

Maintenance Rule. That is, the plant staff will assess and manage risk, and define compensatory measures as appropriate. In accordance with the philosophy for permitting limited duration inoperability of equipment, the available redundant HPSI subsystem provides adequate defense-in-depth during the period when one HPSI subsystem is inoperable. Additional guidance to critically evaluate simultaneous outages of multiple simultaneous component inoperabilities in conjunction with a HPSI subsystem further enhances defense-in-depth by ensuring the potential to core cooling are adequately controlled. Therefore, the proposed revision to TS 3.5.2 and its associated Bases is acceptable as it maintains an adequate risk-based margin to safety while avoiding unnecessary shutdown risks to repair low risk or risk insignificant inoperabilities, which may be incurred if the revision were not approved.

5.0 REGULATORY ANALYSIS

5.1 Applicable Regulatory Requirements/Criteria

The proposed changes have been evaluated to determine whether applicable regulations and requirements continue to be met.

Regulatory Guide (RG) 1.177 (Reference 13) indicates that for permanent TS changes, incremental CDPs of 5.0E-07 per TS entry are considered very small. As illustrated in the JAR (Reference 1), HPSI System inoperabilities should remain within this “very small” region. In this respect, the proposed change to TS 3.5.2 is acceptable.

The process to control resolution of inoperabilities (e.g. repair) will be consistent with NUMARC-93-01 (Reference 11) and its utilization will be tracked to meet the intent of RG 1.174 (Reference 12). Specifically, use of the flexible CT will be controlled to ensure that the resultant cumulative plant risks during the interval beyond the frontstop CT will be maintained within RG 1.174 guidelines (Regions II and III) and maintained below 1.0E-05 / reactor year. In addition, when the overall incremental plant risks fall within a range of 1.0E-06 to 1.0E-05, appropriate compensatory measures or contingency actions will be established to reduce the risk significance of the current plant configuration. Associated guidance for implementation of the proposed TS change will be maintained as administrative guidance under licensee control. When implemented with the appropriate compensatory actions and risk assessment processes, this TS modification will maintain a high level of public health and safety.

The proposed changes do not require any exemptions or relief from regulatory requirements, other than the TS, and do not affect conformance with any GDC. The approval of this change will maintain conformance with 10 CFR 50.36 and 10 CFR 50.65 (Reference 14).

5.2 No Significant Hazards Consideration

The proposed change will revise NUREG 1432, Revision 2, Revised Standard Technical Specifications for Combustion Engineering Plants, Technical Specification (TS) 3.5.2, ECCS – Operating, to provide a flexible Completion Time (CT) and associated Required Actions for inoperabilities related to a single subsystem of High Pressure Safety Injection (HPSI). This change is necessary to avoid unnecessary plant shutdowns and the subsequent incurrence of transition risks due to HPSI subsystem inoperabilities that do not present a significant adverse impact to overall plant risk. In addition, the proposed change implements a portion of the NRC and industry efforts to established risk-based regulation as a tool to enhance the safety and

welfare of the plant and the general public. Furthermore, a restoration period is provided for multiple subsystem inoperabilities provided the 100% ECCS flow equivalent for each train is maintained.

The proposed change has been evaluated as to 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 proposed change does not require any physical change to any plant systems, structures, or components nor does it require any change in systems or plant operations; thus the probability of an accident previously evaluated occurring remains unchanged. The proposed change does not require any change in safety analysis methods or results. Single HPSI subsystem inoperability is considered in existing plant analyses and regulatory criteria with respect to single failure criteria and the risk of extended HPSI subsystem outages are assessed in accordance with the Maintenance Rule. Because risk is appropriately managed and compensatory measures established where necessary, the consequences of an accident previously analyzed are not significantly increased. The change to establish the extended HPSI CT limits is justified because operation within the requirements of the Maintenance Rule continues to be governed by adequate regulation and plant programs.

   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.

   HPSI System inoperabilities are assumed in existing analyses with respect to single failure criteria and are limited by existing regulation. Extending the time in which a HPSI component may remain inoperable does not constitute a change that could result in a new type of accident initiator than that previously identified. In addition, overall plant risk will be managed in accordance with the Maintenance Rule to help ensure continued safe plant operation.

   Therefore, the proposed change does not create the possibility of a new or different kind of accident from any previously evaluated.

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

   Response: No.

The proposed change does not require any change in accident analysis methods or results. Overall plant risks will continue to be appropriately managed and compensatory measures established when appropriate to reduce the overall risk during extended HPSI CT periods. In addition, an evaluation of common cause failure and a determination of the flow capacity of remaining Emergency Core Cooling (ECCS) components will continue to be performed in relation to HPSI System inoperabilities. Although components important to safety have an impact on overall plant risk and may impact the overall margin to safety, the adverse impacts that are realized due to single HPSI subsystem inoperabilities is largely offset by the avoidance of unnecessary shutdown transition risks and the establishment of compensatory measures and contingency actions where appropriate.

Therefore, the proposed change does not involve a significant reduction in a margin of safety.

Based on the above, the proposed amendment presents 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.

6.0 ENVIRONMENTAL CONSIDERATIONS

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.

7.0 REFERENCES

1. WCAP-15773, "Joint Application Report for the Implementation of a Risk Management Technical Specification for the High Pressure Safety Injection (HPSI) System," June 2002.

2. "Risk Informed Technical Specification: Project Description," NEI, June 2001.

3. TSTF 358, Revision 6, "Missed Surveillance Requirements," September 2001.

4. TSTF 359, Revision 6, "Increase Flexibility in Mode Restraints," October 8, 2001.

5. LER #94-005-01, Palo Verde Unit 2.

6. CE-NPSD-593, "Partial Response to NRC Generic Letter 89-19: Small Break LOCA Recovery with Low Head HPSI," CEOG Task 651, CE Owners' Group, October 1990.

7. CENPSD-1045-A, "Joint Application Report: Modifications to Containment Spray System Technical Specifications," CE Owner's Group, March 1998.

8. CE-NPSD-996, "Joint Applications Report: Emergency Diesel Generator AOT Extensions," CE Owner's Group, June 1995.

9. CE-NPSD-1168-A, Revision 00, “Joint Applications Report for Containment Isolation Valve AOT Extension,” CE Owner’s Group, January 2001.

10. CE-NPSD-1184-A, Revision 00, “Joint Application Report for DC Power Source Allowed Outage Time Extension,” CEOG, May 2001.

11. NUMARC-93-01, Revision 3, “Industry Guidelines for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants,” NEI, July 2000.

12. RG 1.174, “An Approach for using Probabilistic Risk Assessment in Risk Informed Decisionmaking on Plant Specific Changes to the Licensing Basis,” USNRC, July 1998.

13. RG 1.177, “An Approach for Risk Informed Decisionmaking: Technical Specifications,” USNRC, August 1998.

14. 10 CFR 50.65, Appendix A, “Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," NRC, July 10, 1991 (56FR41324) and July 19, 1999 (64FR38551)

15. NRC Memorandum to V. Stello, Jr., from R. L. Baer, "Recommended Interim Revisions to LCOs for ECCS Components," December 1, 1975.

16. IE Information Notice No. 87-01, January 6, 1987.

3.5 EMERGENCY CORE COOLING SYSTEMS (ECCS)

3.5.2 ECCS - Operating

LCO 3.5.2 Two ECCS trains shall be OPERABLE.

APPLICABILITY: MODES 1 and 2,
MODE 3 with pressurizer pressure ≥ [1700] psia.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
--- **- REVIEWER'S NOTE -** The adoption of this Condition is contingent upon implementation of a program to perform a contemporaneous assessment of the overall impact on safety of proposed plant configurations prior to performing and during performance of maintenance activities that remove equipment from service. ---		
A. One LPSI subsystem inoperable.	A.1 Restore subsystem to OPERABLE status.	7 days
B. One HPSI subsystem inoperable.	B.1 Restore subsystem to OPERABLE status. OR B.2.1 Determine that Completion Time extension beyond 72 hours is acceptable. AND	72 hours 72 hours

CONDITION	REQUIRED ACTION	COMPLETION TIME
B. (continued)	B.2.2.1 Verify that Completion Time extension beyond 72 hours remains acceptable. AND B.2.2.2 Perform risk management actions to make Completion Time extension acceptable. AND B.2.3 Restore subsystem to OPERABLE status.	24 hours from discovery of each configuration change that may increase overall plant risk 24 hours from discovery that Completion Time extension beyond 72 hours is not acceptable 30 days or acceptable Completion Time, whichever is less
CB. ~~One~~Two or more ~~trains~~ subsystems inoperable for reasons other than Conditions A or B.	CB.1 Restore ~~train(s)~~subsystems to OPERABLE status.	72 hours
DC. Required Action and associated Completion Time of Condition A, B, or C not met.	DC.1 Be in MODE 3. AND DC.2 Reduce pressurizer pressure to < [1700] psia.	6 hours 12 hours
ED. Less than 100% of the ECCS flow equivalent to a single OPERABLE train available.	ED.1 Enter LCO 3.0.3.	Immediately

ACTIONS (continued)

B.1, B.2.1, B.2.2.1, B.2.2.2, and B.2.3

With one HPSI subsystem inoperable, action must be taken to restore OPERABLE status within 72 hours or a risk-informed analysis performed to determine that the risk of continued operation in the current plant configuration is acceptable for extending the time of inoperability beyond 72 hours. In addition, this evaluation must be performed following the initial 72-hour period whenever plant configuration changes occur that may result in an overall increase in plant risk. The 72-hour Completion Time is based on an NRC study (Ref. 4) using a reliability evaluation assuming one non-functional HPSI subsystem and is a reasonable amount of time to effect most repairs. However, depending on the plant configuration at the time of the HPSI subsystem inoperability, the risk of continued operation may be justified via a risk-informed analysis that follows the guidance in accordance with 10 CFR 50.65(a)(4) (Ref. 7) and is consistent with NUMARC 93-01, Section 11, Rev. 3 (Ref. 8), as outlined in RG 1.182 (Ref. 9). This allowance is based on justification provided in WCAP-15773 (Ref. 10) and the implementation of risk management guidance consistent with Reference 11. Reference 11 demonstrates that the risk can be managed and describes the analyses and any management actions necessary to utilize the extended Completion Time. Extension of the Completion Time is based on acknowledgement that many HPSI system components are not risk-significant and that adequate tools and controls are in place for evaluating plant risks, implementing risk-informed actions, and making appropriate risk-informed decisions.

The risk-informed Completion Time established by Required Action B.2.1 must be updated whenever equipment is rendered unavailable that may increase the overall plant risk in accordance with Required Action B.2.2.1. The overall assessment of risk performed during the 72-hour Completion Time of Required Action B.2.1 and subsequent assessments performed under B.2.2.1 should include a quantitative evaluation whenever possible. Qualitative evaluations should be performed to enhance assessments performed quantitatively or to determine the overall plant risk when quantitative tools are not available. The overall assessment of risk may credit considerations given to established compensatory measures, contingency actions, and avoidance of shutdown transitional risks, among others. The 24 hour Completion Time of Required Action B.2.2.1 is sufficient to evaluate the risk impact of such configuration changes. Should it be determined that the extended Completion Time is not acceptable, the 24 hour Completion Time of Required Action B.2.2.2 provides time to establish compensatory measures or recover from undesirable plant configurations so that the overall plant risk will remain acceptable while in the extended Completion Time. This 24 hour period is acceptable because risk management actions, such as plant configuration

BASES

ACTIONS (continued)

B.1, B.2.1, B.2.2.1, B.2.2.2, and B.2.3 (continued)

changes, operator training, and process changes are being implemented which will have the effect of reducing plant risk. Regardless of the acceptability of the evaluated risk impact, the inoperable HPSI subsystem must be returned to OPERABLE status within a maximum of 30 days. This maximum limit provides sufficient time to complete repairs while taking into account HPSI system operational goals and provides for return to a configuration as described in the deterministic accident analysis.

~~C~~B.1

If two~~one~~ or more subsystems~~trains~~ are inoperable except for reasons other than Condition~~s~~ A ~~(one LPSI subsystem inoperable)~~or B and at least 100% of the ECCS flow equivalent to a single OPERABLE ECCS train is available, the inoperable components must be returned to OPERABLE status within 72 hours. The 72 hour Completion Time is based on an NRC study (Ref. 4) using a reliability evaluation and is a reasonable amount of time to effect many repairs.

An ECCS train is inoperable if it is not capable of delivering the design flow to the RCS. The individual components are inoperable if they are not capable of performing their design function, or if supporting systems are not available.

The LCO requires the OPERABILITY of a number of independent subsystems. Due to the redundancy of trains and the diversity of subsystems, the inoperability of one component in a train or subsystem does not necessarily render the ECCS incapable of performing its function. Neither does the inoperability of two different components, each in a different train or subsystem, necessarily result in a loss of function for the ECCS. This allows increased flexibility in plant operations when components in opposite trains are inoperable.

An event accompanied by a loss of offsite power and the failure of an emergency DG can disable one ECCS train until power is restored. A reliability analysis (Ref. 4) has shown that the impact with one full ECCS train inoperable is sufficiently small to justify continued operation for 72 hours.

Reference 5 describes situations in which one component, such as a shutdown cooling total flow control valve, can disable both ECCS trains. With one or more components inoperable, such that 100% of the equivalent flow to a single OPERABLE ECCS train is not available, the facility is in a condition outside the accident analyses. Therefore, LCO 3.0.3 must be immediately entered.

ACTIONS (continued)

D.1 and D.2

If the inoperable subsystem(s) cannot be restored to OPERABLE status within the associated Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and pressurizer pressure reduced to < 1700 psia within 12 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power in an orderly manner and without challenging unit systems.

~~E~~D.1

Condition C~~B~~ is applicable with two~~one~~ or more subsystems~~trains~~ inoperable. The allowed Completion Time is based on the assumption that at least 100% of the ECCS flow equivalent to a single OPERABLE ECCS train is available. With less than 100% of the ECCS flow equivalent to a single OPERABLE ECCS train available, the facility is in a condition outside of the accident analyses. Therefore, LCO 3.0.3 must be entered immediately.

BASES

REFERENCES

4. NRC Memorandum to V. Stello, Jr., from R. L. Baer, "Recommended Interim Revisions to LCOs for ECCS Components," December 1, 1975.

5. IE Information Notice No. 87-01, January 6, 1987.

6. CE NPSD-995, "Low Pressure Safety Injection System AOT Extension," April 1995.

7. 10 CFR 50.65(a)(4).

8. NUMARC 93-01, “Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants,” Revision 3.

9. RG 1.182, “Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants,” May 2000.

10. WCAP-15773, “Joint Application Report for the Implementation of a Risk Management Technical Specification for the High Pressure Safety Injection (HPSI) System,” August 2002.

11. Risk Management Technical Specifications, Risk Management Guide

ATTACHMENT 1

Westinghouse Proprietary Class 2

WCAP-15773-P
Revision 00

September 2002

Joint Application Report for the Implementation of a Risk-Managed Technical Specification for the High Pressure Safety Injection (HPSI) System

CEOG Task 1175

L E G A L N O T I C E

This report was prepared as an account of work sponsored by the CE Owners Group and Westinghouse Electric Company, LLC. Neither Westinghouse nor the CEOG, nor any person acting on their behalf:

A. Makes any warranty or representation, express or implied including the warranties of fitness for a particular purpose or merchantability, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or

B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of, any information, apparatus, method, or process disclosed in this report.

WCAP-15773-P, Rev 00

Joint Applications Report for the Implementation of a Risk-Managed Technical Specification for the High Pressure Safety Injection System

CEOG Task 1175

September 2002

Author: Raymond E Schneider
Raymond Schneider
Probabilistic Safety Analysis

Approved: RC Whipple
Richard Whipple
Probabilistic Safety Analysis

COPYRIGHT NOTICE

ABSTRACT

This document justifies the implementation of a Risk-Managed Technical Specification (RMTS) modification to Technical Specification 3.5.2, "ECCS Operating of NUREG-1432, "Standard Technical Specification for CE Plants." The RMTS both maintains the present Technical Specification structure and allows for the risk-informed control of HPSI system outages consistent with the intent of 10 CFR 50.65 Maintenance Rule. The intent of the RMTS is to allow "at power" plant operation for "extended" times (compared to current Completion Times) when the equipment outage is managed utilizing 10 CFR 50.65 processes and evaluated in accordance with 10 CFR 50.65(a)(4) and associated guidance. Overall, the net impact of the RMTS will be risk neutral as the risks of continued operation would be offset by implementation of contingency actions and by avoidance of transition risks. The aggregate risk impact of the implementation of RMTSs will be managed in accordance with the requirements of 10 CFR 50.65, the plant Performance Indicators, and the reactor oversight process (NUREG-1649). The aggregate risk will be tracked in a manner consistent with limiting annual risk increments in accordance with RG 1.174.

SUMMARY

In response to the NRC and industry initiative to improve plant safety by developing Risk-Informed Technical Specifications, the Combustion Engineering Owners Group (CEOG) has undertaken a program for defining and obtaining Risk-Informed Technical Specification (TS) improvements. As part of this program, several technical specification Completion Times Surveillance test frequencies and Required Actions were identified for joint action.

This report provides support for risk informing the Technical Specifications associated with the Emergency Core Cooling System in order to allow continued power operation beyond the current Completion Times for conditions when one High Pressure Safety Injection train is partially degraded. To effect this goal, a Risk-Informed Technical Specification is proposed which provides for use of the Maintenance Rule processes to assess and manage plant risk following the expiration of the HPSI train Completion Time. Depending on the risk significance of the HPSI train inoperability, Completion Time is allowed to increase to up to 30 days. In order to control plant risk, the integrated incremental core damage and large early release probabilities during this time interval should be maintained consistent with the guidance of NUMARC-93-01 Rev. 03 for quantitative or "blended" maintenance rule implementations. In addition, the incremental accumulated risks associated with the risk-informed Technical Specification will be tracked in order to limit accumulated risk in the extended Completion Time consistent with the guidance of RG 1.174. The intent of this Completion Time extension is to enhance overall plant safety by avoiding potential unscheduled plant shutdowns and avoiding unnecessary plant and regulatory burden in the generation of Notice of Enforcement Discretion. In addition, this extension provides for increased flexibility in scheduling and performing maintenance and surveillance activities. The risk control processes recommended for the High Pressure Safety Injection system are generic and can be applied to other systems contained in the TS. This effort is being pursued as a joint CEOG activity.

Generic information supporting this change, as well as the associated plant specific information to demonstrate the impact of these changes on an individual plant basis is provided. The supporting/analytical material contained within the document is considered applicable to all CEOG member utilities regardless of the category of their plant's TSs.

Risk assessments presented in this report provide examples of the use of Probabilistic Safety Assessment tools to manage risk. Analyses provided are based upon plant Probabilistic Safety Assessment models that adequately reflect the plant configuration during normal operation.

The justification for this request was based on an integrated review and assessment of plant operations, deterministic/design basis factors and plant risk. Results of this study demonstrate that the proposed Completion Time extension provides plant operational flexibility while allowing plant operation with an acceptable level of risk. The expected risk impact of this Technical Specification change, including implementation of associated administrative processes, will be minimal.

TABLE OF CONTENTS

TABLE OF CONTENTS

APPENDICES

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES, Continued

LIST OF ACRONYMS

AFW	Auxiliary Feedwater
AOT	Allowed Outage Time
CDF	Core Damage Frequency
CDP	Core Damage Probability
CCDF	Conditional Core Damage Frequency
CCF	Common Cause Failure
CCW	Component Cooling Water
CE	Combustion Engineering
CEOG	Combustion Engineering Owners Group
CM	Corrective Maintenance
CT	Completion Time
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EOP	Emergency Operating Procedures
FCS	Fort Calhoun Station
HPSI	High Pressure Safety Injection
ICDP	Incremental Core Damage Probability
ISTS	Improved Standard Technical Specifications
LCO	Limiting Condition of Operation
LERF	Large Early Release Frequency
LOCA	Loss of Coolant Accident
LPSI	Low Pressure Safety Injection
MOV	Motor Operated Valve
NOED	Notice of Enforcement Discretion
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
OOS	Out of Service
PM	Preventive Maintenance
PORVs	Power Operated Relief Valves
PSA	Probabilistic Safety Assessment
PVNGS	Palo Verde Nuclear Generating Station
PWR	Pressurized Water Reactor
RG	Regulatory Guide
RITS	Risk Informed Technical Specification
RMTS	Risk Management Technical Specification
RCS	Reactor Coolant System
RWT	Refueling Water Tank
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SONGS	San Onofre Nuclear Generating Station
TS	Technical Specification
TSTF	Technical Specification Task Force

1.0 PURPOSE

The purpose of this report is to document a Risk-Managed approach to permit flexible outage periods when complying with Technical Specification (TS) Allowed Outage Times (AOTs). An application of this approach is provided for the High Pressure Safety Injection (HPSI) System. Specifically, this report provides the results of a pilot evaluation of the feasibility of risk informing selected High Pressure Safety Injection (HPSI) System Required Actions within the plant Technical Specifications (TSs). The process to manage the risk during an extended outage requires that the acceptability of continued power operation be confirmed. This report supports a risk-informed modification to the TS (e.g., Improved Standard Technical Specification (ISTS) 3.5.2 "ECCS-Operating") which provides actions to be taken when one HPSI train is declared inoperable and repairs cannot be completed within the existing AOT Completion Time (hereafter called the "frontstop AOT"). A maximum AOT of 30 days, known at the "Backstop AOT" will provide a limit to the time any TS component, regardless of risk, may remain inoperable. The frontstop and backstop AOTs are the constituent parts of the flexible AOT approach.

This AOT/CT extension will provide needed flexibility in the performance of preventive and corrective maintenance during power operation. The backstop AOT serves as a pilot example of how risk-informed processes may be integrated into the TS and maintenance process to provide a risk-informed means of plant configuration control and work prioritization. Justification is based on an integrated review and assessment of plant operations, deterministic/design basis factors and plant risk. With implementation of concomitant risk assessment processes, the proposed TS change will enhance plant operational flexibility with an acceptable impact on plant risk. Controls on this process ensure that use of the backstop portion of the flexible AOT will not significantly impact the plant risk profile or result in an after-the-fact change to the plant design basis.

This TS change is consistent with the objectives and the intent of the Maintenance Rule (10 CFR 50.65, Reference1). Specifically, 10 CFR 50.65(a)(4) requires a risk-informed assessment prior to removing equipment from service for preventive maintenance and upon entry into a corrective maintenance condition. This requirement applies to all risk significant components, regardless of their TS designation. It is the intent that upon entry into the backstop portion of the AOT/CT of the Risk Managed Technical Specification (RMTS), regardless of the cause, risk will be managed via risk assessment and control processes consistent with the Maintenance Rule; including the general guidance for performing risk assessments contained within NUMARC-93-01, Section 11 (Reference 2). Processes recommended to support the risk assessment beyond the frontstop AOT/CT are summarized in Appendix B. The resulting TS will be identified as a Risk-Managed TS reflecting the importance of risk management in its development.

This page intentionally blank.

2.0 SCOPE OF PROPOSED CHANGES TO TECHNICAL SPECIFICATIONS

The proposed Technical Specification change revises the existing AOT/CT requirement for the operability of the HPSI subsystems of the Emergency Core Cooling System (ECCS). Specifically, it is proposed that TS Action Statement(s) be included for conditions when a single inoperable HPSI train cannot be returned to service within the approved (i.e. frontstop) TS AOT/CT. The frontstop AOT/CT for a HPSI train for Combustion Engineering (CE) designed Pressurized Water Reactors (PWRs) varies from 1 day to 7 days.

The primary intent of the AOT/CT extensions is to demonstrate that risk-informed processes may be used to assess low risk conditions resulting from various maintenance activities. Such activities can be safely extended beyond the frontstop AOT/CT, should a low risk repair/activity require an extended time. It is envisioned that this risk management TS will obviate (or significantly reduce) the need for a Notice of Enforcement Discretion (NOED) and risk-inform the plant shutdown determination process. This flexibility will ensure that low risk system degradations that would cause a train to be declared inoperable can be managed and repaired/resolved in a risk-informed manner.

The process to control resolution of inoperabilities (e.g. repair) will be consistent with NUMARC-93-01 (Reference 2) and its utilization will be tracked to meet the intent of Regulatory Guide (RG) 1.174 (Reference 3a). Specifically, use of the flexible AOT/CT will be controlled to ensure that the resultant incremental plant risks during the interval beyond the frontstop AOT will be maintained within RG 1.174 guidelines (Regions II and III). Associated guidance for implementation of the RMTS will be maintained as administrative guidance under licensee control. When implemented with the associated compensatory actions and risk assessment processes, these TS modifications will maintain a high level of public health and safety.

This page intentionally blank.

3.0 BACKGROUND

In response to the NRC's initiative to improve plant safety by risk-informing the technical specifications, the Combustion Engineering Owners Group (CEOG) in cooperation with the nuclear industry has undertaken a program to identify features of the plant TSs that would benefit from a risk-informed approach. This effort is part of an eight-tiered initiative established by the nuclear industry in 1999 (Reference 4).

Limited scope risk-informed TS improvements have already proposed by the industry. These include an improvement to the process of treating missed TS surveillances - Technical Specification Task Force (TSTF) 358 (Reference 5), and elimination of selected mode restraints on less risk significant components - TSTF 359 (Reference 6). This aspect of the industry Risk-Informed Technical Specification effort, identified in Reference 4 as Initiative 4B, focuses on the change to selected TSs that would allow continued “at power” plant operation under conditions when the component cannot be returned to service in the defined fixed (“frontstop”) AOT provided an assessment ensures continued plant operation with acceptable risks. In essence, this TS change merges the plant’s configuration control and maintenance programs with the Maintenance Rule (10 CFR 50.65) and TS Action Statements. Design basis configuration control is ensured by the availability of the backstop AOT.

The HPSI system has been selected for this pilot implementation effort (See TS 3.5.2, “ECCS,” of NUREG-1432). This TS is selected for three reasons. First, the HPSI system is a highly risk-significant ECCS mitigation system for PWRs and hence must be carefully monitored. Second, the HPSI system has numerous components reflecting multiple system functions and mitigation capabilities; thus degraded performance or partial inoperabilities within a train does not imply a complete loss of mitigation by the affected train. In fact, many issues that would result in a declared inoperability of a HPSI train may not be risk significant. Finally, the system has many components and valves that require periodic maintenance and surveillance. Non-risk significant degradations of HPSI train components have lead to a forced shutdown (Reference 7) at one CE designed PWR and potential shutdowns at others.

The intent of the Backstop TS change is to enhance overall plant safety by avoiding unnecessary risk associated with unscheduled plant shutdowns. In addition, this TS change provides for increased flexibility in scheduling and performing maintenance and surveillance activities.

This report provides generic information supporting these changes, as well as the necessary plant specific information to demonstrate the impact of these changes on an individual plant basis. All CE designed Nuclear Steam Supply System (NSSS) plants are participating in this CEOG activity. The supporting/analytical material contained within this document is considered applicable to all CEOG member utilities regardless of the category of their plant TSs. The proposed TS structure and control processes are only discussed with respect to changes to TS 3.5.2; however, they are applicable to any standby mitigating system TS.

Risk assessments provided in this report are based upon plant Probabilistic Safety Assessment (PSA) models that reflect the various plant operational configurations.

This page intentionally blank.

4.0 SUMMARY OF APPLICABLE TECHNICAL SPECIFICATIONS

There are three distinct categories of Technical Specifications at CE designed NSSS plants.

The first category is called the Standard Technical Specifications (STS). Through February 1996, NUREG-0212, Revision 03 (Reference 8), referred to as "Standard Technical Specifications," provided a model for the general structure and content of the Technical Specifications originally approved for most CE NSSS plants. Plants currently using NUREG-0212 TSs include Millstone Unit 2, St. Lucie Units 1 & 2, Arkansas Nuclear One Unit 2 and Waterford Steam Electric Station Unit 3.

The second category corresponds to the Improved Standard Technical Specifications (ISTS) guidance provided in NUREG-1432, Revision 2, dated April 2001 (Reference 9). CE designed PWRs that have implemented or are implementing the ISTS format include Calvert Cliffs Units 1 and 2, Palo Verde Units 1, 2 and 3, San Onofre Units 2 and 3 and Palisades.

The last category includes those TSs that have structures other than those outlined in either NUREG-0212 or NUREG-1432. These TSs are generally referred to as "custom" technical specifications and are associated with the early CE designed PWRs. Currently, the only CE designed NSSS that uses "custom" TSs is Fort Calhoun Station (FCS).

Each of these three categories of TSs includes operating requirements for the HPSI system.

4.1 STANDARD TECHNICAL SPECIFICATIONS

The requirements for HPSI system are contained in the requirements for ECCS trains/subsystems in the standard technical specifications of NUREG-0212, Revision 03 and NUREG 1432, Revision 2. Each of these documents provides separate ECCS requirements depending upon the plant operating mode.

Requirements that are Applicable to Power Operation

The more restrictive requirements are applicable when the plant is in an operating mode where the presence of a single active failure must be considered in the design basis accident analysis. The applicable modes for these more restrictive requirements are (a) power operation (Mode 1), (b) startup (Mode 2) and (c) hot standby (Mode 3), all of which occur at high RCS pressures. The TS changes proposed in this document apply to Modes 1, 2 and high-pressure Mode 3 operation. (HPSI system requirements are reduced to the availability of one HPSI train for low pressure in Mode 3 and Mode 4 operation.)

The specific standard technical specifications for the applicable Modes are Limiting Condition for Operation (LCO) 3.5.2 of NUREG-0212, Revision 03 and LCO 3.5.2 of NUREG-1432, Revision 2. In LCO 3.5.2 of NUREG-0212, Revision 03, two independent Emergency Core Cooling System (ECCS) trains are required to be Operable. For the applicable plant operating modes, each ECCS train is required to include one operable HPSI pump. In comparison, for

these same plant operating modes, LCO 3.5.2 of NUREG-1432 addresses two redundant, 100% capacity ECCS trains, each consisting of HPSI and Low Pressure Safety Injection (LPSI). Hence, any maintenance or surveillance test that would render a HPSI train inoperable would also result in the inoperability of the corresponding ECCS train.

Both TS 3.5.2 of NUREG-0212 and TS 3.5.2 of NUREG-1432 allow continued power operation with a single inoperable ECCS train for a maximum of 72 hours. Hence, if a single ECCS train is inoperable due to preventative or corrective maintenance on a HPSI train, the train must be restored within 72 hours (including the operability of the affected HPSI train). If this train was not restored to an operable status within this period of time, other TS requirements would direct that the plant be placed, within a specified time period, in an operating mode where alternate operability requirements for ECCS are met.

4.2 "CUSTOMIZED" TECHNICAL SPECIFICATIONS

Customized TSs for the ECCS trains differ from the standard TSs of both NUREG-0212 and NUREG-1432. These differences include: (a) the duration of the specified AOT, (b) the link between the HPSI train and other ECCS trains and components and (c) the details of the action statements when LCO requirements are not met. Presently in the CE plant fleet only FCS employs a customized set of TSs. For FCS, the defined AOTs for an out-of-service HPSI train during power operations is 24 hours.

5.0 SYSTEM DESCRIPTION AND OPERATING EXPERIENCE

5.1 SYSTEM DESCRIPTION

The HPSI system is an integral part of the ECCS. The primary function of the HPSI system is to inject high pressure borated water into the RCS following loss of inventory and reactor overcooling events. Additionally, for some CE plants, the HPSI system can be used for RCS cooling via feed and bleed emergency procedures.

Variations in the HPSI system design and performance characteristics exist among CE designed PWRs. Table 5.1-1 provides a comparison among CE designed HPSI Systems. At a minimum, the CE designed PWR HPSI system consists of two (2) HPSI pumps that inject water from a borated water source into the RCS. Many CE designed PWRs include three HPSI pumps with the third pump considered to be an installed spare or "swing" pump. One or more HPSI pumps are required to be operable via the applicable TS. Borated water can be directly injected into the RCS from a Refueling Water Tank (RWT) (which is located outside of containment) or recirculated (once the RWT is depleted) from the containment building sump. Typically, the operable HPSI pumps are maintained in standby and may be actuated either manually or automatically via indications of either high containment pressure or low pressurizer pressure. Automatic actuation of ECCS components is triggered by generation of a Safety Injection Actuation Signal.

HPSI pumps in CE designed NSSSs have shutoff heads that range from ~1170 to 1900 psig. Use of the medium pressure HPSI pumps provides performance capability sufficient to ensure inventory makeup to the RCS following all sizes of Loss of Coolant Accidents (LOCAs) (Reference 10). Injection into the RCS is possible at several cold and hot leg locations; however only cold leg injection is automatically initiated during the early phase of a LOCA. Hot leg injection is manually initiated late in the larger-break LOCA sequences. Simultaneous hot and cold leg injection is required late in large LOCA sequences to prevent possible boric acid precipitation within the reactor core.

System Operation

A. Safety Injection and Recirculation

The HPSI system provides borated water to the RCS following loss of inventory events, such as a LOCA or Steam Generator Tube Rupture (SGTR) and following severe overcooling transients such as those resulting from a Main Steam Line Break or Feedwater Line Break.

For CE designed PWRs, HPSI pumps are maintained in a standby state. Following a plant upset, safety injection may be actuated by generation of a Safety Injection Actuation Signal. Safety injection can also be manually initiated. Upon receipt of a Safety Injection Actuation Signal, the HPSI pumps are automatically started and the cold leg loop injection valves are opened. If the RCS pressure is above the HPSI pump discharge head, the HPSI pump then recirculates the safety injection water from the borated water source through minimum recirculation valves until the RCS pressure becomes low enough to allow flow into the RCS. For smaller LOCAs the RCS

pressure may remain above the HPSI pump shutoff head. To ensure proper pump operation when the RCS pressure is above the pump shutoff head, a mini-flow line is maintained opened to recirculate HPSI flow to the RWT.

In the mode of cold leg injection, the HPSI pumps draw water from a stored borated water source (such as the RWT). Each HPSI pump discharges into one of two high pressure injection headers. Outflow from each of the headers is directed to the four RCS cold legs via four independent injection lines.

Prior to depletion of the injection water source, the suction of the HPSI pumps is automatically switched to the containment building sump. The Containment Spray System (CSS) and/or the containment fan coolers provide containment heat removal. The HPSI system in conjunction with the containment heat removal system provides long term cooling capability for the core following large and intermediate sized LOCAs.

The necessity for HPSI pump cooling varies among the CE designed PWRs and is dependent on HPSI design, size and placement. All HPSI pumps typically can deliver injection flow (from the RWT) without special cooling requirements. Following depletion of the RWT, the HPSI system is reconfigured to inject recirculated water from the containment ECCS sump. Whereas RWT water is typically less than 100^{o}F, the water in the containment ECCS sump may reach in excess of 250^{o}F. During the HPSI recirculation mode of operation, containment cooling is normally required to ensure adequate Net Positive Suction Head (NPSH) and prevent HPSI pump cavitation. HPSI pump cooling is required to ensure that the HPSI motor does not overheat. HPSI motor cooling is typically provided via a portion of the auxiliary building Heating, Ventilation and Air Conditioning (HVAC) system or by mixing sump fluid with cooled CSS water. For some older units, the HPSI pump design and placement are such as that the pump can satisfactorily operate in recirculation mode without special cooling requirements.

Long term cooling of the reactor core and the RCS for the smaller LOCAs is accomplished via the Shutdown Cooling (SDC) System. For larger LOCAs, long term cooling involves use of the HPSI and/or the LPSI (plant dependent) to simultaneously inject into the RCS hot and cold legs of the primary system (see below).

B. Hot Leg Injection

Following a large or medium LOCA, and after the RWT (or similar tank) is depleted, borated water is recirculated via the HPSI through the cold-leg injection lines. For a LOCA with a break in the cold-leg piping, part of the safety injection flow is diverted through the break and part of the flow is injected into the core. Since the system cannot remain pressurized, the reactor vessel upper head, outlet plenum and Steam Generator (SG) tubes void. Steam formed in the core flows through the SG tubes and to the break location. Boric acid is left behind in the reactor vessel. If this continues without intervention, the boric acid concentration in the reactor may eventually increase beyond the solubility limit. Boric acid may then precipitate and interfere with coolant circulation and heat removal. This problem does not occur for a large LOCA initiated from the RCS hot leg as liquid flows through the core prior to flowing out of the break and allows flushing of the boric acid.

The consequences of boric acid precipitation remain uncertain. However, the problem of boric acid precipitation is avoided by implementing proceduralized actions to realign the Safety Injection (SI) flow to both the hot and cold-legs within many hours up to about 1 day (precise time is plant dependent) following the event initiation. The hot-leg injection flow flushes the core and thus limits the boric acid concentration in the core region. All CE designed plants with the exception of Calvert Cliffs Units 1 & 2 and St. Lucie Unit 2 rely entirely on the HPSI pumps to establish hot leg injection.

C. Once-Through Core Cooling ("Feed and Bleed")

In addition to providing design basis safety functions, for some CE designed plants the HPSI System, in conjunction with the Power Operated Relief Valves (PORVs) or ECCS Vent valves, can function to provide a backup core cooling mechanism for transients where steam generator heat removal is inadequate. (This mechanism is not credited in the safety analysis of record, the analysis corresponding to applicable Updated Final Safety Analysis Reports.) In this application, operators are instructed in the plant specific Emergency Operating Procedures (EOPs) to depressurize the RCS and align the HPSI system for feed-and-bleed cooling. The technical basis for the viability of feed and bleed as a heat removal success path is discussed in References 13a and 13b. The treatment of feed and bleed cooling as a success path within the PSA is presented in the Individual Plant Examination (IPE) submittals.

Feed and bleed cooling is available to all early generation CE designed PWRs. Feed and bleed cooling is not available to San Onofre Units 2 and 3, Waterford Unit 3 and Palo Verde Units 1, 2 and 3. These units are designed without PORVs or ECCS Vent valves on the pressurizer. To enhance recovery from severe loss of feedwater events, these later units have instituted procedures for responding to a total loss of Feedwater (FW) event that includes use of the startup feedwater pumps and/or, aggressive steam generator depressurization to allow the use of condensate pumps, or use of the firewater system for secondary side makeup.

D. Mitigation of Steam Generator Tube Ruptures (SGTRs)

During a SGTR event, a break occurs in a steam generator tube, and primary side inventory is lost to the steam generator. The CE EOP guidance requires the operators to stabilize the leak to < 50 gpm. In the early phase of the SGTR, event inventory makeup may be provided via the HPSI system. In the long term, charging flow from the Chemical and Volume Control System will be sufficient to maintain the core covered while the plant is depressurized and heat removal transitioned to the shutdown cooling system.

Table 5.1-1
Comparison of HPSI System Functions for CE Designed PWRs

Plant	No. of HPSI Pumps	Approx. HPSI Shutoff head (psi)	Spare HPSI Pump Powered by either EDG	HPSI Supports Feed & Bleed	Required for Hot Side – Cold Side Injection[8]		Comment
					Y/N	Time/Hrs	
Palisades	2	1170	Not Applicable	Yes	Yes	6	Third HPSI pump supplied in original design converted to spare AFW pump.
Ft. Calhoun (Reference 16a)	3	1380	N (See comment)	Yes	Yes	8.5	Current TS requires operability for all 3 HPSI pumps. Two pumps are aligned to one EDG.
Calvert Cliffs Units 1&2 (Reference 16b)	3	1257	Y	Yes	No	8-11	
Millstone Point 2 (Reference 16c)	3	1170	Y	Yes	Yes	8-10	Third HPSI pump connected to swing 4160 VAC bus aligned to one of two emergency buses. Re-alignment may take up to 45 minutes.
St. Lucie Unit 1 (Reference 16d)	2	1170	Not Applicable	Yes	No	4 to 6	Installed spare initially available at unit has been abandoned (Reference 16d)
St. Lucie Unit 2 (Reference 16d)	2	1170	Not Applicable	Yes	No	4 to 6	See Note 5
ANO-2 (Reference 16e)	3	1450	Y	Yes	Yes	4	See Notes 1, 5, 7
Waterford Unit 3 (Reference 16f)	3	1450	Y	No	Yes	4	See Notes 2, 3, 4, 5
San Onofre Units 2 & 3 (Reference 16g)	3	1450	Y	No	Yes	8	See Notes 2, 5
Palo Verde Units 1, 2 & 3 (Reference 16h)	2	1900	Not Applicable	No	Yes	2	See Notes 2, 5, 6 HVAC provided via essential room coolers (air cooling coil and fan). Loss of HVAC alarmed. Backup cooling proceduralized.

Notes:

1. ECCS Pressurizer Vent System used as alternative "bleed" path for "feed and bleed" cooling.
2. Response to total loss of FW events includes proceduralized aggressive secondary side cooldown and condensate or firewater injection into the steam generator. Allows potential use of LPSI to backup HPSI.
3. Third HPSI pump is supplied from a swing AC power bus that can be powered by either EDG. Because of the potential for plant trips when realigning the swing AC bus, bus alignment is not performed during normal operation. During accident conditions, the third HPSI pump could be powered from either EDG if necessary.
4. Feedwater system is highly reliable. Backup to MFW includes injection from the Emergency Feedwater and Startup FW pumps. Injection of startup feedwater into the steam generator does not require depressurization.
5. Safety Injection Tank (SIT) pressure approximately varies between 500 and 650 psig. Supports aggressive cooldown.
6. HPSI pump can run dead headed for ~ 20 minutes.
7. Two room coolers required to keep pump cool during recirculation cooling.
8. No differentiation is made between hot and cold side breaks.

5.2 OPERATING EXPERIENCE

5.2.1 Preventive Maintenance (PM)

Many CE designed PWRs include an installed spare HPSI pump in the plant design. When the spare HPSI pump can be powered by either the engineered safeguard bus or when the spare HPSI is powered by the same engineered safeguard bus as that for the maintained system, use of the installed spare as a replacement for one of the other two HPSI pumps allows extended pump maintenance to be performed on a HPSI train without entering an LCO Action Statement.

The plant is required to enter an LCO Action Statement when less than two trains of HPSI are available. The inoperability of a HPSI train may be caused by maintenance activities on an associated pump and/or valve(s). Plants with a spare HPSI pump must enter an LCO Action Statement when maintenance is performed on a HPSI train due to inoperability of a HPSI pump and the spare HPSI pump cannot be used to replace the inoperable HPSI pump. Plants without a spare HPSI pump must enter an LCO Action Statement when maintenance is performed on a HPSI train due to inoperability of a HPSI pump. Other maintenance activities that require declaration of the HPSI train as inoperable include maintenance on HPSI injection valves, mini-recirculation line components, hot side injection valves and associated automatic actuation signals[1].

Consistent with the Maintenance Rule (10 CFR 50.65(a)(4)), the plant risk associated with the current plant configuration will be assessed and any necessary restrictions will be placed on concurrent out of service equipment prior to entry into the Action Statement. In addition, a work plan is typically developed for completing the associated maintenance within an acceptable period that is normally shorter than the duration of the frontstop AOT.

Many types of preventive maintenance on HPSI train components (including post-maintenance verifications and tests) require a period of less than 24 hours. However, some activities such as seal replacement may require several days of maintenance. Preventive maintenance of HPSI components "at power" is generally associated with either a HPSI pump or system valve. Typical activities associated with PMs for a HPSI pump include:

- Change of oil and filter
- Lubrication
- Replacement/Tightening of seals
- Bearing replacement

In general, the most extensive anticipated on-line preventive maintenance activity in the HPSI system is that associated with Motor Operated Valves (MOVs) and/or Air Operated Valves

[1] Plants that must voluntarily enter the LCO Action Statement for HPSI pump PM are Palisades, St. Lucie Units 1 and 2, and Palo Verde Units 1, 2 and 3. Ft. Calhoun Station is equipped with a spare HPSI pump, however, electrical bus alignment limitations restrict the use of the pump to a single defined ECCS subtrain. Waterford 3 powers the third HPSI via a "swing" AC bus which may be powered by either emergency DG. During normal operation, including maintenance activities, Waterford 3 administratively restricts the alignment of the "swing" AC bus to a single emergency DG. This restriction is imposed in order to limit the possibility of a plant trip due to realignment. During accident conditions, the swing AC bus can be powered by either emergency DG. HPSI system maintenance on the HPSI pump train requires entry into the LCO Action Statement.

(AOVs). Most HPSI systems contain between 15 and 20 MOVs/AOVs. Depending on the plant, the HPSI system MOVs can be located either inside or outside of containment. HPSI system MOVs include pump mini-flow recirculation valves, HPSI header and hot/cold leg injection valves and discharge isolation valves. Preventive maintenance activities associated with valves within the HPSI system include:

- Valve Overhaul
- Valve Repacking

Typically, pump PMs require less than 24 hours to complete and valve PMs can generally be performed in 8 hours or less. When performed properly and no unknown pre-existing failure is uncovered, PM and post maintenance testing on a single HPSI System component can be completed within the 72 hour (frontstop) AOT which is available to most CE designed NSSSs.

5.2.2 Surveillance Testing of HPSI System Valves

Surveillance testing of valves (MOVs, AOVs and check valves) in the HPSI system occurs as a result of In-Service Test Program (IST), TS requirements or periodic verification of valve actuator setup as required by Generic Letter 89-10. The scope of these tests vary based on the type of valve, specific activity and utility procedures. The interval for in-service testing is defined via the TSs. This testing may be performed either at power or during a plant shutdown. In the case of the testing of the MOVs at power, it is required that the MOV stroke time be within a specified band and that the valve operator performance be within defined limits. Since this test can be performed so as to minimally disable a portion of the HPSI system, its actual impact on risk is negligible. The test is conducted so as to not disable the valve's ability to receive and respond to an Engineered Safety Features Actuation Signal. Thus, the actual time interval that the tested valve is either not functional, or in its design basis event response position, is very small.

5.2.3 Corrective Maintenance (CM)

Corrective maintenance in the HPSI system involves both pump and valve repair. In practice, the term corrective maintenance is typically used for the repair of a component resulting from an emergent observable malfunction which may or may not compromise the ability of the system or component to perform its safety function. This terminology can place corrective maintenance on HPSI pumps due to small oil/water leaks (which do not necessarily impair SI system function) into the same category as more extreme failures, such as a debilitating pump motor failure.

CE designed NSSS units have mean HPSI pump repair times of under 24 hours, with the longer repair times taking in excess of 72 hours. It is expected that failures that render the HPSI pump non-functional will be skewed to the longer repair times. Parts accessibility may also impact the repair time. Since existing failures may be diagnosed following a component surveillance, the time for diagnostic and repair may be insufficient for the existing LCO to assure task completion prior to exceeding the AOT/CT. In practice, in order to optimize plant Performance Indicators, it is expected that many plants will reduce the total time of entry into a LCO Action Statement by interchanging the spare pump with the pump required for maintenance. For circumstances when

a spare pump is unavailable, maintenance that exceeds the frontstop AOT/CT will result in plant shutdown or the exigent generation of a NOED. The flexible AOT concept may avoid plant shutdown by allowing continued operation provided the risk consequences of extended operation are acceptable.

MOVs and/or AOVs in the HPSI system also require occasional corrective maintenance. The corrective maintenance may involve the valve actuator and/or the valve itself. Post-maintenance testing of these valves involves detailed testing procedures. During the corrective maintenance and post-maintenance testing, the Action Statement and the associated AOT is entered and the valve is declared inoperable. In order for the valve actuator to be considered operable, the valve actuator characteristics must be demonstrated to be within specified bands of torque and thrust. In order for the valve itself to be considered operable, it may be necessary to conduct a flow test in addition to other valve related tests (i.e. stroke time, etc.). If these tests provide unacceptable results, the MOV is still considered inoperable and further corrective maintenance must be performed within the remainder of the AOT. Failure to repair and re-diagnose the valve as operable would result in the applicability of other LCO action requirements to bring the plant to a shutdown mode within a relatively short period of time or development of a Justification for Continued Operation. Past testing at a CE designed NSSS unit has resulted in at least one case where the repair and testing of a malfunctioning MOV was completed within one hour of the expiration of the 72 hour AOT. In 1994, another CE designed NSSS unit was required to shutdown when repair of a HPSI MOV could not be completed in 72 hours (Reference 7).

5.2.4 Operability vs. Functionality

In many instances a HPSI train may be declared inoperable even though the system is partially or entirely functional. Such conditions exist when inoperabilities affect a specific system parameter, availability of an automated system feature or a redundant component, etc. For the HPSI system partial system inoperabilities include (but are not limited to) the following:

- Unavailability of one or more HPSI delivery lines,
- Unavailability of auto start capability on a single HPSI train,
- Unavailability (partial or complete) of HPSI recirculation capability for a single HPSI train,
- Partial or complete inoperability of the HPSI mini-flow recirculation lines,
- Unavailability of cooling to HPSI pump room cooling, or
- Degraded HPSI delivery flow.

The above inoperabilities have risk impacts from negligible to small and therefore inability to complete a repair within the assigned AOT/CT of the TS action statement should not force the initiation of the plant shutdown process.

In practice, for low risk situations associated with the aforementioned repairs, plants often avoid the shutdown consequence by developing the technical basis to obtain a NOED. In other instances repairs are delayed or inefficiently scheduled to avoid an unintentional shutdown. It is the intent of the flexible AOT/CT TS to allow more efficient scheduling of low risk maintenance and to reduce the scheduling and resource burdens associated with generation of a NOED for

assessed low risk conditions when a controlled plant centered process with appropriate contingency actions adequately manage plant risk.

5.2.5 Related Licensing Actions

Over the past five years, numerous applications have been presented to the NRC to establish risk-informed AOTs for a variety of systems and components. Approvals to extend the AOT for an inoperable LPSI train or an inoperable SIT were obtained for many CE designed PWRs as part of a Risk Informed CEOG TS improvement activity.

Risk informed AOT extensions were also approved separately for inoperability of one Emergency Diesel Generator (EDG), inoperability of one train of CSS, inoperability of selected Containment Isolation Valves (CIVs), and inoperability of one battery and associated battery charger (See References 17a, 17b, 17c, & 17d). These AOT/CT extensions established risk-informed fixed AOTs/CTs, with the intent that risk accumulation in these intervals would be controlled via a configuration control maintenance program. These programs have been integrated into the plant's Maintenance Rule process. HPSI unavailability is tracked and reported as a performance indicator under the NRC's Reactor Oversight Process.

6.0 TECHNICAL JUSTIFICATION FOR RISK INFORMED MODIFICATIONS TO THE HPSI AOT AND ACTION STATEMENTS

This section presents an integrated assessment of the proposed change to the TSs. The focus of the assessment includes motivation and the need for technical specification change, the impact of the change on the plant design basis event and a probabilistic risk assessment. This TS structure is intended to be a pilot for similar Risk Managed Technical Specification (RMTS) changes associated with most other component related TSs. The discussion here focuses on the HPSI system. However, the concepts proposed in this pilot are applicable to TSs of other emergency systems.

Section 6.1 presents a summary statement of the need for the AOT/CT extension. The supporting information for this section has been previously presented in Section 5. Section 6.2 provides an assessment of deterministic factors, particularly those associated with the plant design basis. Section 6.3 establishes the potential risk impact associated with implementing the proposed technical specification change. Risk insights and compensatory actions applicable to the proposed TS modification are summarized in Section 6.4. Guidance associated with implementation of RMTS is presented in Appendix B.

6.1 STATEMENT OF NEED

The proposed TS change will create a new ISTS 3.5.2 Condition B or its equivalent to include actions for continued plant operation when the frontstop AOT cannot be met. A proposed TS compatible with the ISTS, which includes the backstop AOT feature, is presented in Table 6.1-1. The actions of this table include a risk assessment that demonstrates that the risk of continued operation is acceptable. An expanded discussion of the proposed change is presented in Section 7. A proposed modification to the associated TS is presented in Appendix A.

Much of the maintenance performed on a HPSI train requires the train to be tagged out for periods of less than one day. However, in some instances, corrective and/or preventive maintenance of a HPSI pump and valves and testing of valves may require taking one train of the HPSI system out of service for more than several days. Recent experience has included a case where an MOV repair and post repair dynamic testing were completed within one hour of the expiration of the AOT. In another recent example, a plant shutdown was initiated when the time required for an MOV repair was anticipated to exceed the allowed completion time (Reference 7). Thus, repair of HPSI system components within the existing AOT/CT cannot be guaranteed and may result in an unscheduled plant shutdown. A less restrictive AOT/CT would allow the plant to complete maintenance activities at power while avoiding a potentially greater risk associated with plant shutdown.

Table 6.1-1
Example of Proposed Technical Specification

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
B. One HPSI train inoperable.	B.1	Restore inoperable HPSI train to OPERABLE status.	72 hours
		OR	
	B.2.1	Determine that the risk configuration is acceptable for completion time extension beyond 72 hours.	72 hours
		AND	
	B.2.2	Determine that the risk configuration is acceptable for continued operation beyond 72 hours.	Whenever configuration changes that affect plant risk occur
		AND	
	B.2.3	Restore inoperable HPSI train to OPERABLE status.	Acceptable completion time extension or 30 days, whichever is less.

6.2 ASSESSMENT OF DETERMINISTIC FACTORS AND DEFENSE IN DEPTH

6.2.1 Thermal-Hydraulic Considerations

6.2.1.1 LOCA

In the early 1970's, the NRC defined deterministic acceptance criteria (10 CFR 50.46, Reference 12) and prescriptive guidance (Appendix K to 10 CFR 50) for evaluating the performance of the ECCS following a LOCA.

The ECCS acceptance criteria from 10 CFR 50.46 are as follows:

a. Maximum fuel element cladding temperature is $\leq$ 2200ºF;

b. Maximum cladding oxidation is $\leq$ 0.17 times the total cladding thickness before oxidation;

c. Maximum hydrogen generation from a zirconium water reaction is < 0.01 times the hypothetical amount that would be generated if all of the metal in the cladding cylinders surrounding the fuel, excluding the cladding surrounding the plenum volume, were to react; and

d. The core is maintained in a coolable geometry.

In order to meet these acceptance criteria, the designs of CE designed NSSS ECCS have included the following elements:

1. A high pressure safety injection capability for providing delivery of coolant to the RCS during the early phase of the blowdown process, and matching boil-off to maintain inventory during the later phases following reflooding of the core;

2. A passive safety injection capability provided via SITs providing a one time, rapid inventory injection into the RCS as the RCS depressurizes below the tank pressure; and

3. A low pressure coolant injection capability for providing high mass flow to the RCS at low RCS pressures.

These design elements and the corresponding system operability requirements in the TSs have been based on a limiting design basis accident scenario. This limiting scenario considers LOCAs up to the size of a full offset shear double ended guillotine break of the primary coolant piping in combination with a loss of offsite power and the "worst" single equipment failure.

To cope with the large loss of RCS inventory during a large LOCA, an ECCS consisting of a train of water injection systems was devised. For CE designed PWRs, the components of the ECCS typically included four (4) passively actuated SITs, two redundant HPSI trains and two redundant LPSI trains. The SITs were designed with the task of rapidly providing liquid

inventory to reflood a voided core. The role of the HPSI pumps was primarily to supply inventory for smaller LOCAs and provide long term inventory control and core "flushing" for the large break LOCAs. Once the primary pressure decreases below the LPSI shutoff head, the LPSI pump can provide inventory control and long term heat removal via the Shutdown Cooling (SDC) System.

Both the HPSI and LPSI systems are designed to operate in the injection and recirculation modes. In the injection mode, borated inventory is taken from an external water source and directly injected into the RCS. Once the inventory in the external tank is depleted and the inventory is relocated in the containment, the water is recirculated from the containment sump to the RCS. Adequate sump water cooling may be maintained via the Containment Heat Removal System (CHRS) and/or SDCS heat exchangers.

The plant design basis requires that the plant be able to cope with the full spectrum of LOCAs. Design basis calculations indicate that the requirements of 10 CFR 50.46 can be met in the context of Appendix K provided that a minimum of one HPSI train (plus other ECCS components dependent on break size) respond to all LOCAs. Availability of a HPSI train during the most limiting LOCAs may not preclude fuel damage since limited fuel damage (localized balloon ruptures at hot spots) may occur due to short duration flow stagnation and core uncoveries that may occur during the event.

In addition to responding to ruptures of primary or branch line piping, the HPSI trains may also provide inventory makeup following an event leading to stuck open PORVs or Pressurizer Safety Valves (PSVs), or leaks of the RCP seal.

More realistic analyses indicate that, depending on the details of the RCS depressurization and performance of the LPSI system, HPSI may not be required for mitigation of large LOCAs. This is not of significant consequence as the likelihood of these LOCAs are very low (~5.0E-06 or less per year; See for example Reference 20). For smaller LOCAs, PSA analyses using the realistic evaluation model (Reference 22) indicate that during the injection-mode core damage conditions may be avoided with HPSI flow rates less than minimum design basis requirements.

6.2.1.2 Steam Generator Tube Rupture (SGTR) Events

The HPSI system provides inventory control during the design basis SGTR event with or without a concurrent loss of off-site power. The design basis of this event requires the HPSI system to maintain the core covered with water at all times. One HPSI train is sufficient to satisfy the design basis safety function.

6.2.1.3 Overcooling Transients

During severe overcooling events such as a Main Steam Line Break or a Feedwater Line Break, the HPSI supplements the Reactor Protective System and the Chemical and Volume Control System and contributes boration to the core. In this manner the HPSI system contributes to maintaining a subcritical core (See Reference 13b). In the design basis context, one HPSI train is

sufficient to provide adequate responses to overcooling transients. PSAs performed for CE designed PWRs consider these overcooling events as low probability precursors to core damage.

6.2.1.4 Feed and Bleed Cooling

Many CE designed PWRs include once-through-core-cooling (or Feed and Bleed cooling) in their emergency operating procedures (See Table 5.1-1). This represents a non-design basis risk-significant application of the HPSI system. "Feed and Bleed" cooling is an alternative method for core and reactor plant system heat removal for use in situations where the feedwater to the steam generator is lost for an extended time period. The Feed and Bleed scenario may develop following the diagnosis of a complete loss of feedwater event. In this event, the operator is instructed via the Emergency Operating Procedures (EOPs) to manually vent the pressurizer and to make up lost inventory from the RCS by feeding the RCS via the HPSI pumps. In this cooling mode, inventory to the RCS is controlled via HPSI injection and pressurizer venting. EOP strategies for once-through-cooling typically direct that pressurizer venting be performed via the Power Operated Relief Valves (PORVs) or in the case of ANO-2, the ECCS vent valves.

Provided PORVs are opened in accordance with plant EOPs, one HPSI train is sufficient to accomplish adequate core heat removal (See Reference 13a).

6.2.1.5 Comments Regarding PWRs without Feed and Bleed Potential

As was discussed in Section 5.1, several later generation CE designed PWRs are designed without pressurizer PORVs or similar device for controlled venting of the RCS. These plants include San Onofre Units 2 and 3, Waterford Unit 3, and Palo Verde Nuclear Generating (PVNGS) Units 1, 2 and 3. EOPs for these plants do not include feed and bleed techniques as a potential backup for the auxiliary feedwater system. Instead, following a loss of main and auxiliary (or emergency) feedwater systems these plants include procedures for aggressive cooldown of the secondary side. Initiation of aggressive cooldown establishes continued RCS heat removal via injection of makeup water from alternate sources including the condensate system, startup feedwater system or if possible the fire protection system. PVNGS also includes aggressive cooldown procedures for trying to utilize LPSI system to backup HPSI system. While the LPSI pumps are operated at very low RCS pressure, the SIT makeup will provide RCS inventory while the primary and secondary side are sufficiently depressurized.

6.2.1.6 Summary

The HPSI system is an important mitigating system. Availability of the redundant trains (and associated support and actuating systems) during the equipment outage provides protection from the aforementioned plant upset conditions.

6.2.2 Radiological Release Considerations

Extending the AOT for the HPSI system may result in an increase in the unavailability of that system. The redundant train remains capable of performing the system's safety function provided the support systems required to operate the available equipment are operational.

6.2.2.1 LOCA and Other Loss of Inventory Events

The design basis calculation of radiological consequences of a large LOCA are based on a combination of very conservative assumptions intended to ensure that the health and safety of the public is preserved in the event of a maximum hypothetical core melt scenario. The Maximum Hypothetical Accident results in significant and sustained core uncovery, well beyond the minimum cladding damage possible following a design basis LOCA. The design basis for radiological releases following a LOCA is set forth in 10 CFR 100, "Reactor Site Criteria", and detailed in SRP 15.6.5, Reference 14. In practice the 10 CFR 100 radiation release criteria are achieved via reliance on the 1962 "source term" outlined in the Atomic Energy Commission Technical Information Document, TID-14844, "Calculation of Distance Factors for Power and Test Reactors" (Reference 15). This "Source Term" was based on a postulated “in vessel” release from an unmitigated large LOCA. This event is also referred to as the Maximum Hypothetical Accident. Additional conservatism in evaluating the impact of the Maximum Hypothetical Accident radiological release is provided by conservatively limiting the maximum decontamination factor that can be credited for iodine removal in the containment building and the use of upper bound atmospheric dispersion coefficient (*X*/Q's) in estimating doses.

As the event assumes an unmitigated LOCA as its basis, HPSI system availability has no impact on the dose assessment. Furthermore, recent PSAs performed by NRC and several utilities have included realistic assessment of the risk of public exposure to unmitigated LOCAs progressing to severe accidents. The general conclusion of these studies is that public exposure is small, provided that the containment structure remains intact. Containment integrity may be preserved by minimal containment heat removal using either containment sprays or containment cooling units.

6.2.2.2 Steam Generator Tube Ruptures (SGTRs)

Following a SGTR, the EOPs provide guidance to maintain RCS inventory using various means for inventory control. Under these conditions, core uncovery is not expected and radiological releases will not exceed the 10 CFR 100 allowable limits. Redundant HPSI trains and alternate depressurization and mitigation strategies provide a high level of confidence that defense in depth is maintained.

6.3 ASSESSMENT OF RISK

6.3.1 Overview

The purpose of this section is to provide an integrated assessment of the overall plant risk associated with the adoption of the proposed flexible TS modification. As the flexible TS requires a risk assessment to be performed on-line and associated accident management actions to be taken dependent on the existing plant state, the calculations presented in this section are illustrative of the level of risks that may be expected during various HPSI system inoperabilities, and the overall risk assessment process.

In this evaluation, a risk assessment of the HPSI system flexible AOT extension is performed for a range of HPSI train inoperabilities. Specifically, the assessment considers "at power" operational risks associated with partial or complete unavailability of a HPSI train for conditions with and without other system concurrent maintenances. For completeness, this report also considers the impact of external events and the potential for mode transition risks associated with a plant shutdown.

RG 1.177 (Reference 3b) indicates that for permanent TS changes, incremental core damage probabilities of 5.0E-07 per TS entry is considered very small. The associated document, RG 1.174 (Reference 3a), indicated that incremental risks in the range of 1.0E-06 to 1.0E-05 per year are also considered small (Region II). This report credits maintenance rule processes for controlling the specific maintenance evolution, and the RG 1.174 guidance for controlling annual risks. Consequently, the overall approach is consistent with Maintenance Rule guidance risk assessment. Furthermore, the associated Maintenance Rule processes will be activated for all entries into RMTSs. Administrative processes available to assess and manage risk will ensure that the impact of this TS modification will result in a risk neutral or small incremental changes in plant risk.

In practice, incremental risks will be managed by limiting Out-of-Service (OOS) time, implementing risk important compensatory measures, periodic tracking and prospective and retrospective risk evaluations of the use of extended flexible AOT.

Operation within the maintenance evaluation will be consistent with the Maintenance Rule. That is, integrated maintenance risks (including components which require repair times beyond the frontstop) will be controlled to an incremental Core Damage Probability (CDP) of less than 1.0E-05 (See Section 4.3.7.2 of Reference 2). In establishing the integrated maintenance risk, the entire maintenance evolution is evaluated for simultaneous outages of plant components, including the component in the flexible AOT. In order to go beyond the frontstop AOT, the allowable incremental risks will be associated with maintenance of the component beyond the frontshop AOT. Incremental CDPs beyond the frontstop AOT will be "targeted" in the range of 1.0E-06 and will be accompanied by compensatory actions, as appropriate. (Typical Risk Management Actions are discussed in Section 11.3.7.3 of Reference 2). The selection of 1.0E-06 as an incremental target risk reflects the approximate level of risk tradeoffs that may be avoided by repair "at power," thus rendering the change effectively risk neutral. Furthermore, risks of this level or below are considered small. Such levels would ensure low risk impact,

consistent with RG 1.174 and represent a low risk maintenance activity consistent with RG 1.182 and NUMARC-93-01. Regardless, increased risks may be incurred, however, they would be subject to management scrutiny and need additional risk management actions. High risk conditions will be avoided as large incremental risks could impact the overall plant Core Damage Frequency (CDF), as well as challenge the plant's performance under the Maintenance Rule, and reactor oversight programs.

Section 6.3.2 provides example assessments of the increased risk associated with continued operation with a single HPSI train OOS due to various failure modes spanning the range of minimal degradation to full train non-functionality. The variation in the "at power" risk increments are component specific and the implications for the modified TS are discussed. Example plant specific evaluations were performed by the participating utilities. Representative inoperabilities were evaluated by comparing the time required for the specific HPSI system degradation to accumulate an incremental core damage risk of 1.0E-06. From the perspective of the TS change, the risk increment implies the risk incurred by having the component OOS beyond the frontstop AOT and not the risk of total configuration. The larger configuration the risk remains governed by the Maintenance Rule.

Section 6.3.3 provides a brief discussion of the risk of transitioning the plant from Mode 1 to a lower mode (e.g. Mode 4 with Auxiliary Feedwater (AFW) available) and results of example assessments. The mode transition assumes SGs are properly functioning and RCS heat removal is via the AFW system. The risk of continued "at power" operation may be compared with the risk of proceeding with a plant shutdown.

For completeness, the impact of the modified TS on the plant Large Early Release Frequency (LERF) is assessed. The assessment includes an evaluation of the events leading to large early fission product releases and the role of the HPSI system in the initiation and/or mitigation of those events. A bounding LERF assessment for the HPSI system is provided (See Section 6.3.5).

6.3.2 Assessment of "At Power" Risk

6.3.2.1 Methodology

This section provides assessments of the increased risks associated with continued operation with various inoperabilities associated with a single HPSI train. The evaluation of the "at power" risk increments resulting from an inoperable HPSI train was established on a plant specific basis using an updated version of the PSA nodal for each individual plant.

Significant HPSI system design characteristics are presented in Table 5.1-1; key modeling assumptions are presented in Tables 6.3-1 and 6.3-2. Table 6.3-3 provides a comparison of the HPSI system LOCA success criteria. Several illustrative HPSI train inoperability evaluations were performed. Evaluations considered the impact of "individual system degradations" as well as inoperabilities occurring concurrent with other out of service equipment. HPSI analyses included investigations of single and multiple component inoperabilities. These analyses provide a spectrum of examples that demonstrate that unavailability of many components within a HPSI

train or associated support components results in small risk impact, and that CEOG member PSAs are capable of adequately establishing the associated risks.

Single component inoperability studies investigated a wide range of system inoperabilities including:

1. Complete inoperability of a single HPSI train resulting from a random failure of a HPSI pump (no residual functionality assumed).

2. Declared inoperability of a single HPSI train due to random failure of a high pressure SI header injection valve.

3. Declared inoperability of HPSI subtrain due to nonfunctionality of HPSI pump auto start function (one train only).

4. Declared inoperability of a HPSI train due to inability to operate in the recirculation mode.

5. Declared inoperability of HPSI train due to the anticipated failure of the HPSI pump mini-flow line to function following a HPSI system demand.

6. Declared inoperability of a HPSI train due to a failure to meet minimum design basis delivery requirements (< 20% flow deviation).

7. Declared Inoperability of a single HPSI train due to functional failures of the associated HVAC.

Table 6.3-1
HPSI System Dependencies/Significant Failure Modes

Plant	HPSI Room Cooling Requirement	Mini-Flow Operability Requirement
Palisades	Not Required	Without mini-flow HPSI pumps assumed to fail when operated deadheaded for any time interval.
Fort Calhoun Station	Not Required	HPSI pump head is high (~ 1380 psig). Pump vendor indicates that pump can operate for 30 minutes deadheaded w/o mini-flow. Failure of mini-flow will impact a break < 5% of small LOCA spectrum.
Calvert Cliffs Units 1 & 2	(HPSI recirculation CCW cooling only)	Without mini-flow HPSI pumps assumed to fail when operated deadheaded for any time interval.
St. Lucie Units 1 & 2	(HPSI pumped cooled via CCW, HPSI recirculation only)	Without mini-flow HPSI pumps assumed to fail when operated deadheaded for any time interval.
Millstone Unit 2	Required for ECCS recirculation phase only	Without mini-flow HPSI pumps assumed to fail when operated deadheaded for any time interval.
ANO Unit-2	(HPSI recirculation only) (Available provide sump temp. < 280 ^{o}F, Reference 16e)	Not modeled, impact neglected (Reference 16e).
WSES Unit-3	(HPSI recirculation only)	Unavailability of mini-flow assumes HPSI fails for LOCAs and SGTRs.
SONGS Units 2 & 3	HPSI pump motors water cooled via CCW (recirculation only). HPSI pump rooms cooled by Emergency Chilled Water with backup from normal HVAC.	Unavailability of mini-flow assumes failure of very small and small LOCAs
PVNGS Units 1, 2 & 3	(HPSI recirculation only) (Room is alarmed and alternate cooling possible as contingency action (Section 5.2.1.1.9(e) of Ref. 16h)	HPSI can operate dead headed for 20 minutes without mini-flow. (High head discharge indicates no credible failures, Reference 16h)

Table 6.3-2
LOCA Initiating Event Frequencies

Plant	LOCA Initiating Event Frequencies (per year)		
	Small LOCA	Medium LOCA	Large LOCA
Idaho Nuclear Engr Lab Data	5.0E-4	4.0E-5	5.0E-6
Palisades	6.0E-3	3.35E-5	2.0E-4
Fort Calhoun Station	6.8E-3	7.7E-5	7.6E-6
Calvert Cliffs Units 1 & 2**	NA	1.18E-4	NA
St. Lucie Units 1 & 2*	3.01E-3	2.16E-5	5.85E-5
Millstone Unit 2	3.0E-3	1.56E-5	6.8E-5
ANO Unit-2	2.95E-3	6.6E-5	6.79E-5
WSES Unit-3	4.47E-3	1E-3	5.0E -5
SONGS Units 2 & 3*	2.9E-3	7.1E-5	6.5E-6
PVNGS Units 1, 2 & 3	5.1E-4	4.0E-6	5.0E-6

* Very small LOCA category also considered.
** Not available

Table 6.3-3
HPSI System LOCA Success Criteria

	Plant [1]								
Event	**Palisades**	**Fort Calhoun**	**Calvert Cliffs –1 & 2**	**St. Lucie - 1 & 2**	**Millstone Unit 2[5]**	**ANO-2**	**WSES-3**	**SONGS Units 2 & 3**	**PVNGS Units 1, 2, 3**
Injection	1/2 HPSIs to 1/3 intact SI lines	2/3 HPSIs to 1/3 intact SI lines	1/2 HPSIs to 1/3 intact SI lines	1/2 HPSIs to 2/3 intact SI lines	3/4 HPSIs to 3/3 Intact SI lines	1/3 HPSIs to 2/3 intact SI lines	1/2 HPSIs to 2/3 intact SI lines[2]	1/3 HPSIs to 2/3 intact SI lines	1/2 HPSIs to 3/6 SI lines
Recirculation	1/2 HPSIs to 1/3 intact SI lines	2/3 HPSIs to 1/3 intact SI lines	1/2 HPSIs to 1/3 intact SI lines	1/2 HPSIs to 2/3 intact SI lines	3/4 HPSIs to 3/3 Intact SI lines	1/3 HPSIs to 2/3 intact SI lines	1/2 HPSIs to 2/3 intact SI lines[2]	1/3 HPSIs to 2/3 intact SI lines	1/2 HPSIs to 3/6 SI lines
Hot leg [3] Injection	1 HPSI via HL/CL piping	2 HPSI via HL/CL injection piping	HPSI not required	HPSI required for Unit 2.	1 HPSI via HL/CL piping (For CL breaks only)	1 HPSI via HL/CL injection (For CL breaks only)	Late HL/CL entry	1 HPSI via HL/CL injection	1 HPSI via HL/CL piping
	Alignment about 6 hrs	Alignment [4] before 8.5 hrs	Alignment about 8 hrs	Alignment 4 to 6 hrs	Alignment 8-10 hrs	Alignment in 2 to 4 hrs	Alignment not modeled	Alignment 8 hrs	Alignment in 2 hrs

Notes:

(1) Reference 18, Table 1.
(2) Swing pump available via manual action.
(3) Large and medium LOCAs
(4) One HPSI is sufficient for injection requirements. Procedure recommends to address flow balancing concerns.
(5) Data applicable to current MP2 model.

Assessments of component failures were also performed to provide examples of the impact of partial HPSI train degradation in the presence of simultaneous inoperabilities of non-HPSI system components. The inoperable conditions are representative of the spectrum of conditions that may affect a HPSI train during plant operation. HPSI train analysis assumptions for assumed inoperability are discussed below.

A common set of plant-specific analyses was performed in order to demonstrate plant risks associated with partial degration of a HPSI train across the CE fleet. These analyses were performed for a spectrum of PWRs and utilize the current PSA model for the plant. The failures identified above were simulated in each plant's PRA by setting the probability of the affected component to "True." Example incremental plant risks were calculated and the time required to accumulate an incremental risk of 1.0E-06 was identified. The resulting times clearly indicate that many HPSI train degradations resulted in very small incremental plant risks, and in many instances the degraded system "AOT" could far exceed the frontstop AOT value.

Two items should be noted in the assessment process. First, the model utilizes a risk increment of 1.0E-06. This value is selected for illustration. Risks of this level are very small and since transition risks are also of the order of 1.0E-6, the incremental risks of 1.0E-06 may be largely offset by a repair at power which averts the risks associated with transition. Second, incremental risks less than 1.0E-06 are consistent with the guidance for small impact contained in NEI Maintenance Rule guidance (Reference 2) and guidance associated with the reactor oversight process (Reference 19).

The present analysis does not define an incremental CDP value of 1.0E-06 beyond the frontstop as a rigid limit, but rather as a low risk "target." It is expected that risks associated with the entire maintenance will be managed in accordance with Maintenance Rule procedures including guidelines of Section 11.3.7.2 of Reference 2. In the event that maintenance is needed to be performed in the extended AOT/CT and the maintenance requires activity in excess of normal work controls (See Reference 2), then the ICDP associated with the maintenance should be tracked for future assessment. The basis for continued operation in the action statement will be documented and entries will be reviewed.

Note that specific common cause failures are not explicitly considered in the above examples. When entry into the extended AOT (beyond the frontstop) is due to an emergent condition, a common cause evaluation is performed in accordance with the plant corrective action program. If Common Cause Failure (CCF) coupling is anticipated to be significant following the initial investigation, the "at power" risk assessments performed at the time of the outage will consider the impact of CCF in the risk assessment. CCF potential will be identified prior to expiration of the frontstop AOT. Thus, CCF issues will be resolved and/or assessed prior to entry into the extended portion of the Action Statement.

It should also be noted that the times presented in Figures 6.3-1 through 6.3-7 are not AOTs; they are illustrative demonstrations of typical outcomes from the flexible TS process. In practice, risk evaluations will consider the impact of concurrent equipment OOS, as well as qualitative or quantitative assessments of impact of contingency actions or non-PSA modeled plant degradations.

Consequently, specific risk values will not be included in the TS; rather they will be provided as guidelines within internal administrative procedures consistent with the Maintenance Rule. Activities that exceed associated guidelines will receive progressively higher level of management attention.

Section 6.3.2.3 provides example evaluations of incremental CDPs associated with various declared inoperabilities of the HPSI system beyond the frontstop AOT. These analyses utilize the following risk measures:

Conditional Core-Damage Frequency (CCDF): The CCDF is the CDF conditional upon some event, such as the outage of equipment. It is calculated by re-quantifying the PSA model after adjusting the unavailabilities of those basic events associated with the inoperable equipment.

Increase in Core Damage Frequency (ΔCDF): The increase in CDF represents the difference between the CCDF evaluated for the component(s) inoperability and the CCDF evaluated for conditions when the component(s) are not out for test or maintenance. For the HPSI system:

$$\Delta CDF = CCDF_{(1\ HPSI\ degraded/inoperable)} - CCDF_{(HPSI\ operable)}$$

Where,

CCDF = Conditional Core Damage Frequency (per year)

The Incremental Core Damage Probability (ICDP) is calculated as

$$ICDP = \Delta CDF * \Delta T$$

Where ΔT is the time interval under consideration.

The outage time to reach an ICDP of 1.0E-06 can be expressed as:

$$\Delta T_{ICDP} = 1.0E\text{-}6/\Delta CDF$$

The ICDP value of 1.0E-06 represents a threshold typical of a “Small” risk and would not significantly alter the overall plant CDF.

In the following examples, the risk-informed outage time starts upon entry into the extended AOT/CT and represents the time period of incremental CDP due to the HPSI inoperability given the contemporaneous state of the plant.

For purposes of illustration the above outage time is used to demonstrate and compare the impact of various HPSI system inoperabilities. In the above equation, if ΔCDF is in frequency per day, the risk-informed Outage Time will be measured in units of days.

The methodology used to illustrate the above risk impacts is presented in the next section. Assessments below reflect results of current plant specific analyses. Therefore, variations in results will reflect plant design differences and PSA modeling assumptions and scope.

6.3.2.2 Case Description and Example HPSI System Risk Assessments

The CEOG utilities participated in generating example risk assessments. Each of the CEOG utility participants used its current PSA model to assess the CCDF based on the condition that one HPSI train is degraded or unavailable. The PSA model used for the conditional assessment represents the current plant PSA model and in most cases, the current PSA model includes one or more post IPE updates. In addition, all participants in the effort have completed or will shortly complete a PSA peer review using the CEOG Peer Review process (analogous to NEI-00-02, Reference 23). CEOG members are currently participating in a task to have a post issue resolution peer review.

In the current evaluation, the inoperability of the desired component was modeled as follows:

1. Set the basic event probability for the selected basic event failure mode (pump, valve or component or appropriate failure mode) in the inoperable HPSI train, equal to 1.0.

2. Set the basic event probability for the failure mode representing the simultaneous unavailability of the OOS equipment (if any) also to 1.0.

3. Retain basic event probabilities for other failure modes for that train equal to nominal values.

4. Requantify the PSA model.

This Conditional CDF was assessed for PM only. That is, components were removed from service without prior knowledge of a component failure. Under this circumstance, common cause failures were considered as being random events. For emergent repairs due to a component failure, it is expected that the common cause failure probability could increase for a CM condition. The presence of a common cause failure (that would render the redundant components inoperable) will be identified within 24 hours. If as a result of an emergent condition, CCF was found to exist, the redundant HPSI train would be declared inoperable and the plant would enter a more limiting TS. Under these circumstances entry into the region of the HPSI TS beyond the frontstop would not be allowed. The difference between the PM and CM values is a result of the previously mentioned difference in treating common cause failure. Incremental risks are dependent upon the specific HPSI train component failure, which is documented and discussed in Section 6.3.2.3.

Table 6.3-4
HPSI Train Configurations for assumed INOPERABILITY

	Cases					
	1	2	3	4	5	6
Parameter/Inoperability	**One HPSI Pump OOS (PM)**	**One HPSI Injection Line Inoperable**	**Auto. Start Inoperable**	**HPSI Recirculation Inoperable**	**HPSI Injection Flow Degraded (< 20%)**	**HPSI Mini-Flow Valve Inoperable**
HPSI Train	Most limiting HPSI train non-functional	One of 4 SI lines not available*	Auto start inoperable on one HPSI train	HPSI (ECCS sump) Recirc. inoperability	One pump with delivery flow < DB TS Limit	Inoperability of HPSI mini-flow valve affecting one train
Treatment of Common Cause Failure	Random	Random	Random	Random	Random	Random
Plant Status**	Nominal Maintenance	Nominal Maintenance; HPSI Pump functional in affected train	Nominal Maintenance; HPSI Pump functional in affected train	Nominal Maintenance; HPSI Pump operable in injection mode	Nominal Maintenance HPSI Pump otherwise operable	Nominal Maintenance HPSI Pump otherwise operable
Special Assumptions	NA	NA	Actions to increase awareness of need for manual restart not considered	Actions to refill RWT not credited	NA	Impact varies
Status of Second HPSI train	Operable	Operable	Operable	Operable	Operable	Operable

* Does not include line associated with break.
** Assumes random unavailability of all other plant components.

6.3.2.3 Example Assessments of HPSI Train Inoperabilities (Single Component Inoperabilities)

This section illustrates the relative risks associated with the partial inoperabilities of the HPSI system. These assessments demonstrate that PSA tools are adequate to assess and manage risks associated with various levels of HPSI train degradation, and to demonstrate that a high risk system like the HPSI may be declared inoperable for many reasons that have small to negligible risk impact. Two sets of assessments were performed. The first set of analyses represents single HPSI AOT outage assessments with a single inoperable HPSI component. These cases are defined in Table 6.3-4. The second set of analyses investigates the risk of minor HPSI inoperabilities in the presence of risk significant inoperabilities associated with the AFW or an EDG. These later examples were used to demonstrate the impact of multiple simultaneous inoperabilities. Note that in presenting the times associated with the target ICDP, times were limited to a maximum of 30 days based on a limitation imposed in the proposed TS.

6.3.2.3.1 Inoperability of Single Train of HPSI

In this study, various CEOG members assessed the risk impact of the complete inoperability of a HPSI train. Analyses considered total non-functionality of the most limiting HPSI train. For plants with a two-pump HPSI system, this leaves one HPSI train with a single pump available. Plants with three train HPSI systems were analyzed based on normal operational practice. That is, plants with true "swing" pumps would typically realign the spare HPSI pump to the train with the inoperable HPSI pump so that the TS requirement of two independent HPSI trains remains satisfied. Thus, the TS entry would occur only when one HPSI train is inoperable and the swing pump cannot be realigned to that train. This was modeled by assuming the MOV upstream of the SI header was inoperable (See for example WSES-3 and ANO-2 predictions). The spare pump was considered available to the opposite train, in the event of an accident. For plants with rigidly aligned HPSI asymmetries (e.g., Fort Calhoun), the single HPSI pump train was assumed failed, as the likelihood of two inoperable HPSI pumps on the other train was considered remote. All analyses assume a random unavailability of other plant components. Results are presented in Figure 6.3-1 in terms of the number of days required to reach CDP of 1.0E-06. As expected, variations in the predicted time reflect differences in plant alignments, presence or absence of PORVs, and variations in assumed LOCA initiating event frequencies and the assumed role of LPSI as a backup for HPSI (See for example Figure 6.3-1) for selected LOCAs. In general, the results confirm the conservative nature of the 3 day frontstop AOT[2]. It should be noted that under certain plant configurations, especially in the presence of an available swing pump, risks associated with extended operation may remain low (See for example Figure 6.3-1). Plants with more risk significant HPSI dependencies are equipped with PORVs and credit feed and bleed for mitigation of loss of all feedwater events. This is particularly true in the case of Palisades which includes a large PORV that was backfit into its design. In essence, depressurization via PORV and injection via the HPSI provides an effective means of mitigating a loss of feedwater event, thereby further increasing importance of HPSI.

[2] Note that a typical frontstop AOT is generally related to a 5.0E-07 CDP, however the current HPSI AOTs are actually based on system reliability assessments (See Reference 24).

6.3.2.3.2 HPSI Train Inoperability due to Unavailability of one SI Line

This study investigates the risk significance of the unavailability of a SI line. Line unavailability may be due to unavailability or inoperabilities associated with related breakers/relays or valve operators. Such inoperabilities may be uncovered or detected in the course of surveillance tests, or found via design/procurement reviews, system walkdowns, etc. PSA models recognize the fact that LOCA success does not require HPSI injection into all intact cold legs (See Reference 18). Analyses assume that a CCF mechanism that may affect more than one line is not present, although random CCFs are considered. The potential for CCF will be identified within the frontstop AOT. If CCF issues are identified, the correct TS must be entered and appropriate actions taken. (The analyses consider random common cause component or equipment failures.) Results of the evaluation, presented in Figure 6.3-2, show this incremental inoperability to be low risk with times to reach a 1.0E-06 CDP level greater than 30 days.

Actual incremental risks vary from 1.0E-10 to 2.2E-07. Reasons for variability of this outage time estimate are associated with the level of credit given for the use of LPSI (coupled with RCS depressurization) as a backup to failure of the HPSI system, variability of LOCA Initiating Event Frequencies and availability of PORVs. Event success models that require all injection pathways for event mitigation would predict AOTs typical of Figure 6.3-2.

6.3.2.3.3 HPSI Train Inoperability due to Unavailability of HPSI auto start (one train)

This study investigates the impact of unavailability of automatic start capability on one HPSI train. Failure of HPSI autostart was modeled by setting the Fail to Start Basic event to “True” for one HPSI pump or equivalent system basic events. HPSI autostart capability is of primary concern for fast moving transients such as the large or medium LOCAs. Autostart failure may result from inoperability of system relays. Modeling the failure by setting the Failure to Start event to “True” bounds the risk impact as this failure mode includes both mechanical and electrical failures.

Results of this evaluation are captured in Figure 6.3-3. The outage time to reach an incremental HPSI maintenance risk ICDP of 1.0E-06 is shown for several CE designed PWRs. Variations in the risk and calculated outage times are due to variability in the LOCA initiating event frequencies and the degree of manual recovery considered. No specific operator recovery actions are credited. However, typical recovery action may consist of pressing a HPSI start button on the control room panel. Analyses with allowed outage times conservatively modeled the failure to start as affecting the entire ECCS and CS system. Thus, not only was HPSI compromised but so were the LPSI and CS. In all cases no credit was given for prior operator awareness of this particular failure.

6.3.2.3.4 Inoperability of One HPSI Train due to Inability to Operate in the Emergency Sump Recirculation Mode

Figure 6.3-4 compares the risk impact associated with disabling of one train of HPSI to operate in the emergency sump recirculation mode. In this illustration, one train of the HPSI system is disabled such that HPSI recirculation capability cannot be implemented when needed. This failure increases the likelihood of core damage events initiated by large and medium LOCAs.

6.3.2.3.5 Inoperability of One Train of HPSI Mini-flow

A mini-flow line is provided to allow extended deadheaded system operation. Deadheaded operation may occur when the mini-flow valve is closed, a Safety Injection Actuation Signal is generated, and the RCS pressure remains above the shutoff head of the HPSI pump. Extended deadheaded operation of a HPSI pump may lead to pump failure. For deadheaded operation, PSA analysis assumed that mini-flow capability was disabled (e.g. closed mini-flow valve). Results of the study are presented in Figure 6.3-5. The predicted significance of mini-flow capability varies among the units. The significance of mini-flow is dependent on plant design features; specifically, the HPSI pump shutoff head, and the deadheaded operational capability of the pump. In the FCS design, the HPSI pump has a relatively high shutoff head (~ 1380 psig) and low flow delivery, so that the plant can operate with the pump deadheaded for about 30 minutes. This time is sufficiently long so as to significantly limit the range of small LOCAs for which HPSI failure would occur. Operator actions to secure the standby pump are not considered. Similarly, the high head HPSI pumps employed by the PVNGS Units (See Table 5.1-1) are not expected to be required to operate deadheaded for any length of time following a LOCA.

St. Lucie Units 1 and 2 and San Onofre Units 2 and 3 analyses conservatively assume that mini-flow capability is needed to ensure that the HPSI pump is operational for all small LOCAs. WSES-3 and ANO-2 results acknowledge the availability of a swing HPSI capable of backing up a HPSI pump that may fail in deadheaded operation. Since the time the RCS is above the HPSI maximum delivery pressure is short for the wide spectrum of small LOCAs, realignment of the swing HPSI pump later in the event would still ensure inventory control.

6.3.2.3.6 HPSI Inoperability due to Degraded Performance (< 20% head degradation)

Assessments of degraded pump performance were performed using a Realistic LOCA Evaluation Model (Reference 22). At power, identification of a degraded HPSI condition may arise as a result of a design review or similar activity. Since this HPSI test is not normally performed “at power” the declaration will likely not be associated with the surveillance test. These assessments spanned the range of small to the lower end of large breaks. Associated analyses indicate that reductions in HPSI pump injection flows on the order of 80 percent full capacity will still avoid a core damage condition.

For this evaluation the degraded HPSI delivery was modeled as unavailability of a single HPSI injection flowpath. From a thermal-hydraulic perspective the increased resistance associated

with loss of an injection path reduces HPSI injection by approximately 20% (with some design variability). Reduced flow conditions and decay heat (including uncertainties) maintained the post-LOCA peak cladding temperatures below 1500°F. Results of this risk assessment are summarized in Figure 6.3-6.

6.3.2.3.7 HPSI Inoperability due to Failure of HPSI Pump Room Cooling

Based on a plant dependency review it was noted that Palisades and Fort Calhoun have no specific dependency on HPSI equipment cooling during injection or recirculation operational modes. HPSI cooling requirements vary among CE designed PWRs (See Table 6.3-1). This evaluation represents a situation where pump cooling during recirculation is lost either due to a loss of HVAC in the ECCS pump room or the loss of Component Cooling Water (CCW) to the containment spray pump (some plants). The impact of the loss may cause a failure of the associated HPSI pump(s) while operating in the recirculation mode. In general, the impact of HVAC on HPSI operability is small. The variability in results reflects differences in pump design and HPSI relative importance. None of the plants require HPSI pump cooling for successful HPSI performance while in the injection mode. HPSI pumps at Fort Calhoun are relatively low output (due to lower power core) and are designed and positioned to operate in recirculation mode without the need for room cooling. The results of this assessment are presented in Figure 6.3-7.

Extended operation for the repair of this condition may include implementation of procedures and/or features to cool the pump rooms via room fans or other means.

6.3.2.3.8 Summary of Risk Assessments

These assessments confirm the potential benefits and associated small risk of using risk-informed methods to extend HPSI plant operation beyond the “frontstop” AOT when necessary. Using risk-informed approaches to control maintenance, a potential exists for more flexible control and lower risk repairs. As a result of the plants individual risk profile and design, plants are expected to utilize the flexible AOT/CT somewhat differently. Regardless of the plant design and assessment methodology, the plant PSA model can assess the impact of a wide range of low risk HPSI component OOS conditions.

Figure 6.3-1

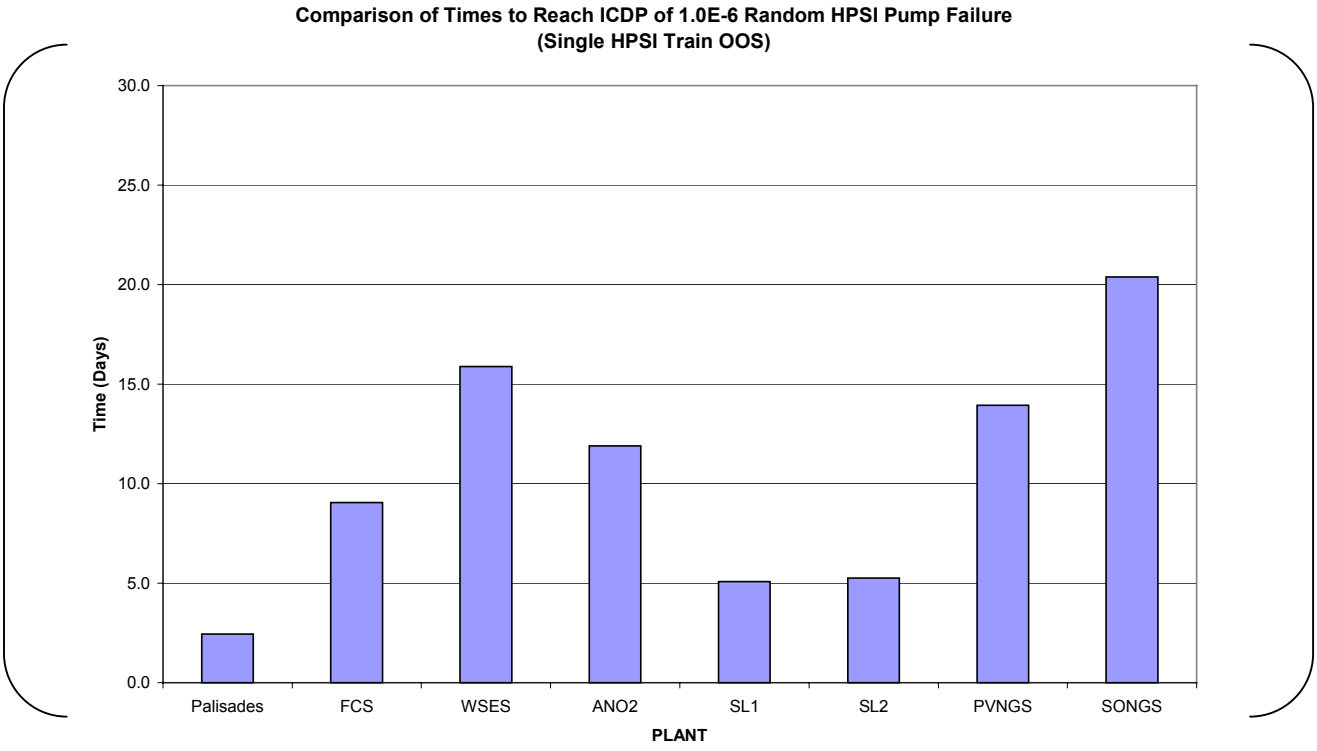


Figure 6.3-2

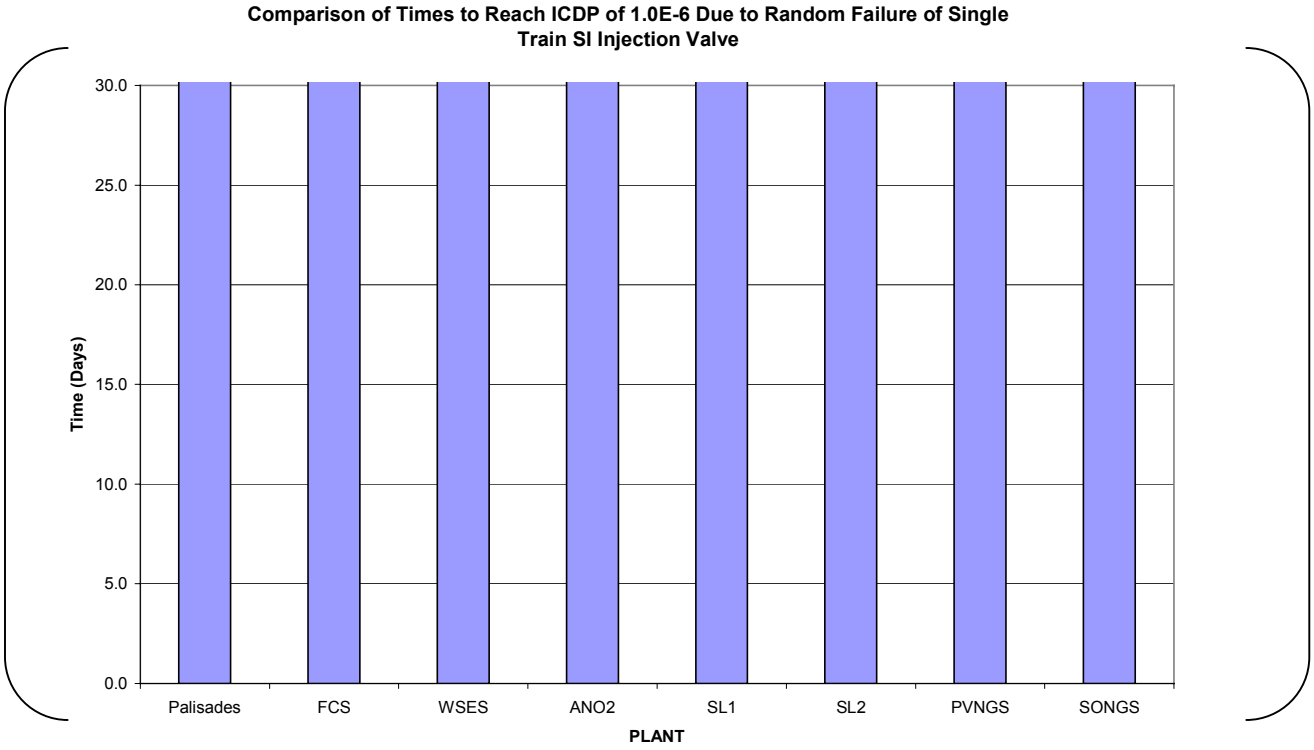


Figure 6.3-3

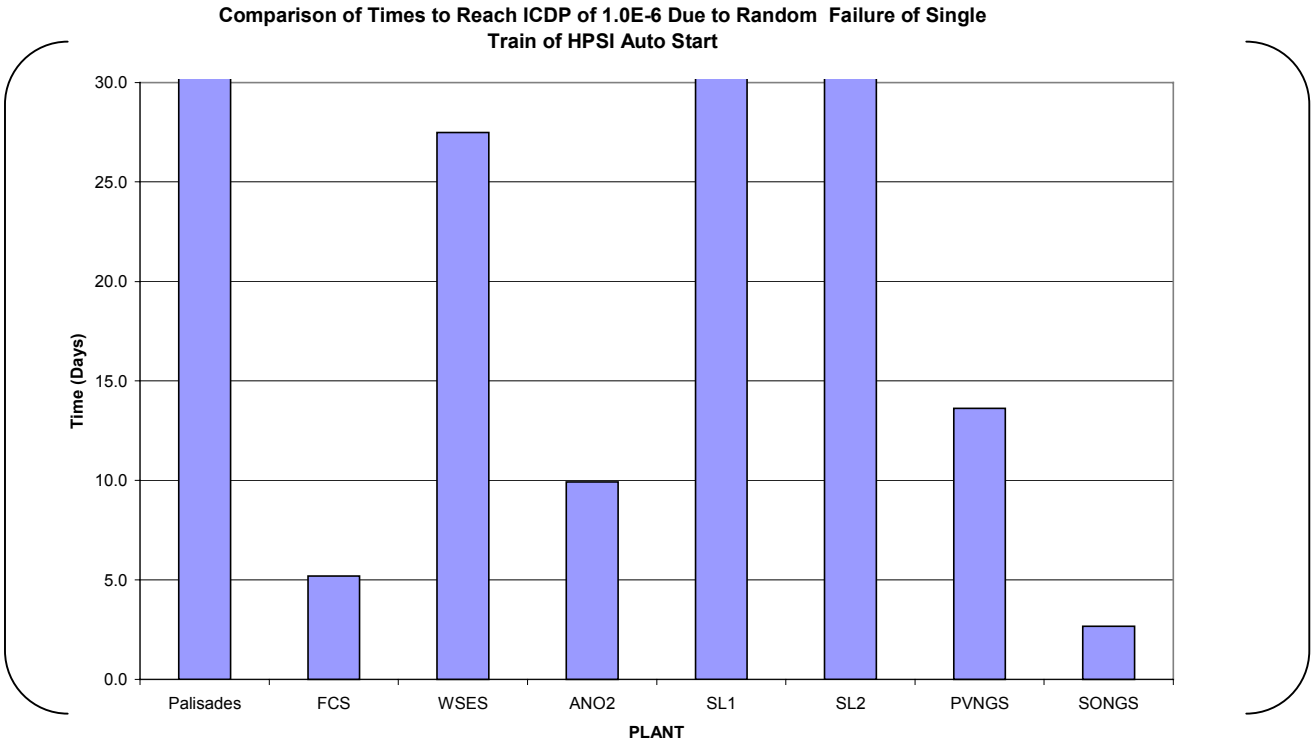


Figure 6.3-4

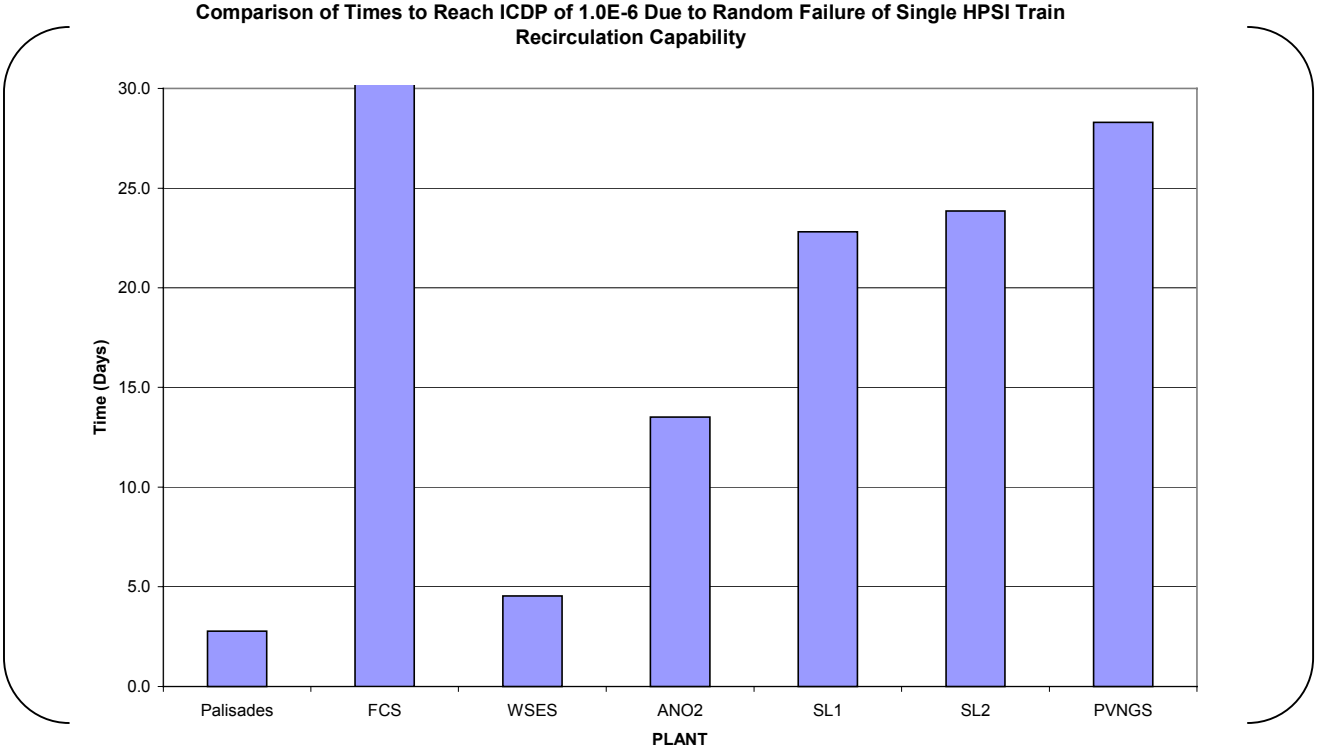


Figure 6.3-5

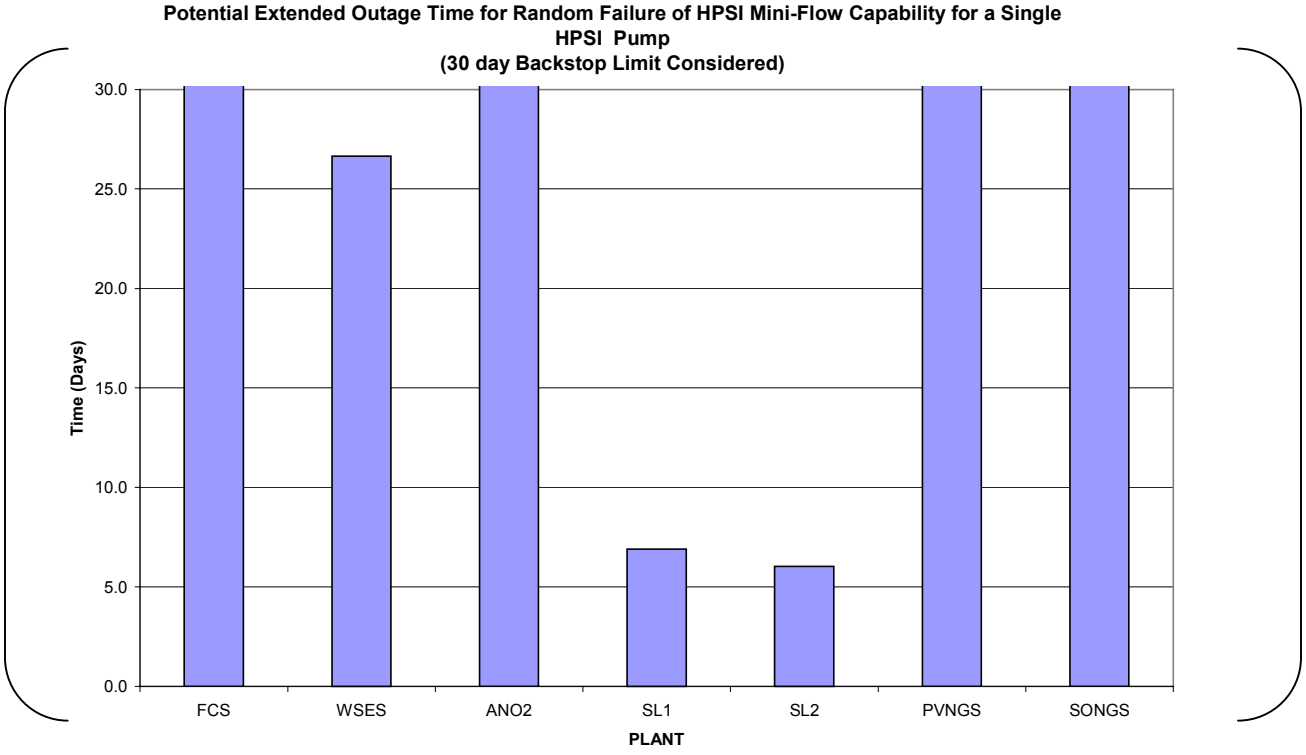


Figure 6.3-6

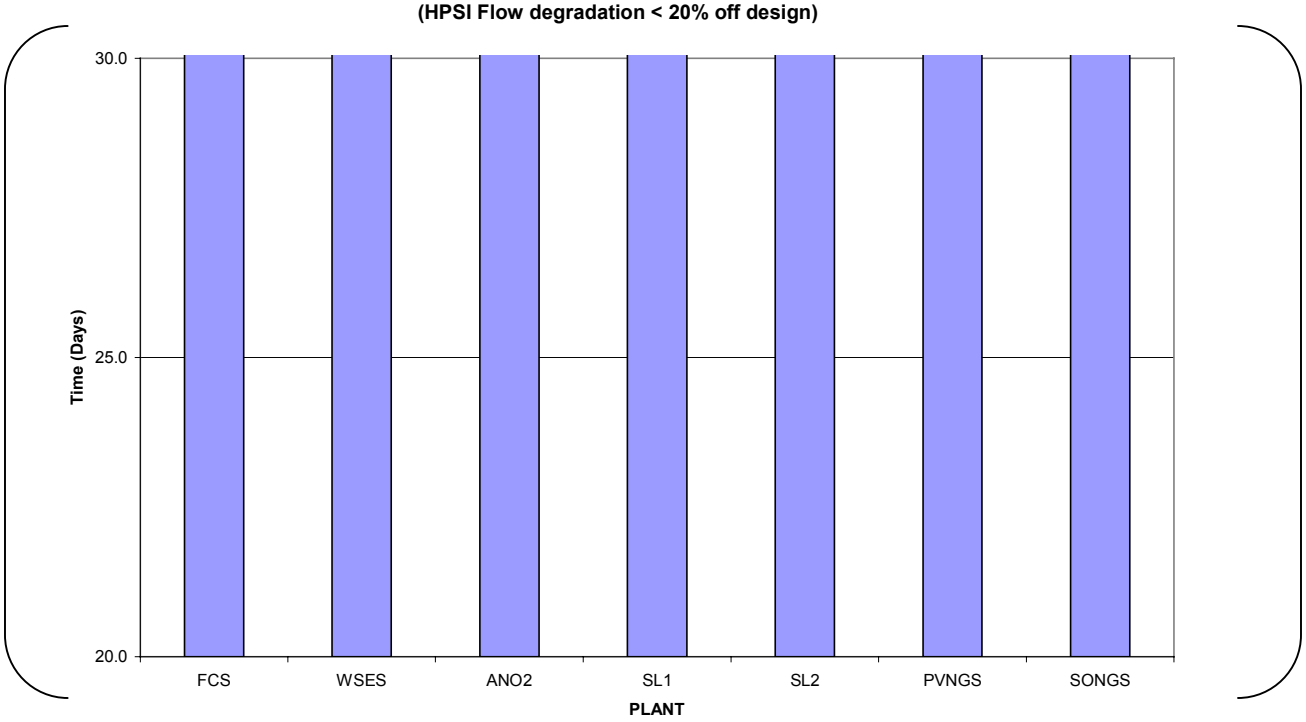
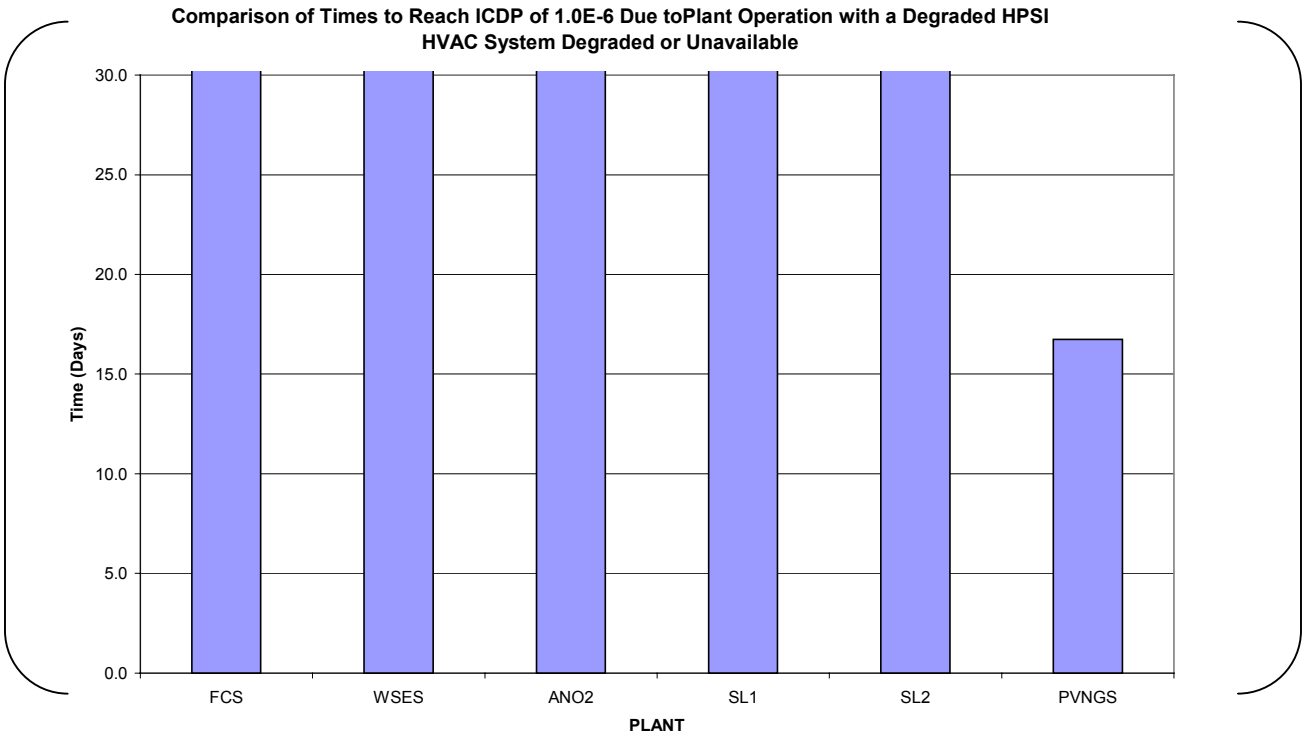


Figure 6.3-7



6.3.2.4 Comments on Risk Ranking of HPSI and Non-HPSI Components

The above discussion provides examples where a single train TS entry, even for a system as highly risk significant as the HPSI may have low risk consequence. SCE performed risk ranking assessment of the PSA modeled components associated with the HPSI system. That study (not shown) indicated that even based on an ICDP threshold of 1.0E-06, only 6% of the HPSI components had a risk level that would result in predicted outage time less than the current 3 day AOT. These components are typically associated with complete inoperability of a single HPSI train (without any swing pump or backup capability considered). Depending on the component that is OOS the associated risk impact of a degraded HPSI system may be negligible. Of the remainder of the components, about 52 % would be clear candidates for a limited duration extension and 42 % would not incur an ICDP risk impact greater than 1.0E-06 even if a full 30 day outage time was utilized (provided concurrent equipment outages did not amplify the importance of HPSI system to plant risk).

6.3.2.5 Impact of Concurrent Maintenance

Table 6.3-5 identifies the cases analyzed involving concurrent maintenance of the HPSI system and another system. In accordance with the Maintenance Rule, the actual maintenance risk will be based on the combined plant configuration using risk-informed Maintenance Rule assessment tools and procedures. That is, according to NEI-93-01, a total configuration ICDP of less than

1.0E-06 implies normal maintenance. For ICDP between 1.0E-06 and 1.0E-05 the plant should use non-quantifiable factors and establish risk management actions. It is also noted that plant configurations with ICDP greater than 1.0E-05 should not be entered voluntarily. Similarly, ILERP guidance should also be followed. However, in this instance the ICDP is evaluated from the zero maintenance plant baseline and includes the risk of simultaneous equipment outage.

Plant risks in the extended AOT/CT associated with the HPSI outage should be tracked when the configuration ICDP exceeds the threshold for normal work controls. Below that threshold, risks are considered acceptably low and special tracking is not required. Above the threshold, tracking should be performed in order to ensure that the accumulated annual risks associated with the use of the extended AOT is less than 1.0E-05 per year and that the extended AOT/CT is properly utilized.

This section evaluates the impact of simultaneous equipment inoperabilities in the presence of a low risk HPSI condition (single SI header line unavailable) with maintenance activities of varying risk consequence. The specific analyses performed and the associated participating plant examples are presented in Table 6.3-5. Results of these analyses are presented in Figures 6.3-8 through 6.3-14. These results clearly show that concurrent unavailabilities would impact overall plant risk and incremental risk of the HPSI inoperability. However, the major contribution to the increased plant risk is the removal of the risk significant component, and not from the accumulation of risk caused by the specific HPSI inoperability investigated. The overall maintenance activity will be controlled via the Maintenance Rule. In the present example the outage time presented is based on a CDP increase of less than 1.0E-06.

A PVNGS study of normal maintenance outages indicated that the incremental core damage worth of the HPSI maintenance operation will vary from negligible for a typical Train B maintenance week to small for a Train A maintenance week (See Figure 6.3-15). Specifically in the PVNGS example, inoperability of a SI valve would increase Train B operational maintenance risk by less than 5.0E-09 per day and Train A maintenance risk by ~ 3.0E-08 per day. The actual risk of HPSI SI line unavailability with a random distribution of OOS components is about 9.0E-10 per day. In this particular example, while the change in risk is notable, the practical risk increment for the flexible AOT is negligible (See Figure 6.3-16). Similar conclusions may be drawn from the Fort Calhoun comparison (See Figure 6.3-8). To ensure the overall plant risk is properly managed, the entries into the extended portion of the AOT/CT will be tracked and its usage evaluated.

Table 6.3-5
Overview of Concurrent Maintenance Analyses

Case ID	Description	Plant								
		Fort Calhoun	Palisades	CC 1 & 2	St Lucie 1 & 2	MP-2	ANO-2	WSES-3	SONGS 2 & 3	PVNGS 1, 2 & 3
1A	One HPSI injection valve OOS with one train of (TD pump) AFW OOS	✓	✓	NA	✓	NA	✓	✓	✓	✓
1B	One HPSI injection valve OOS with one train of (MD pump) AFW OOS	✓	✓	NA	✓	NA	✓	NA	✓	✓
2	One HPSI injection valve OSS with opposite train EDG non-functional	✓	✓	NA	✓	NA	✓	NA	✓	NA
3	One HPSI injection valve OOS with typical plant specific maintenance work week program	✓	NA	NA	✓	NA	NA	NA	NA	✓

NA – Example not available

Figure 6.3-8

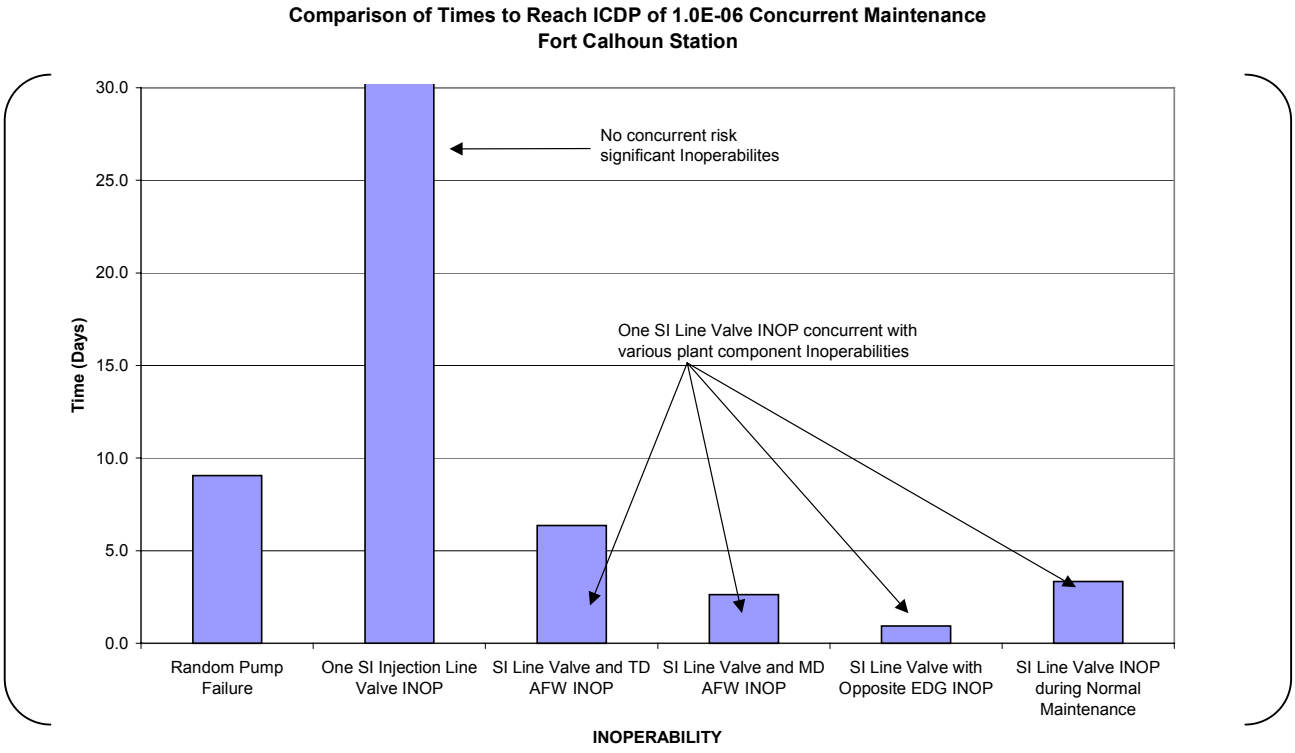


Figure 6.3-9

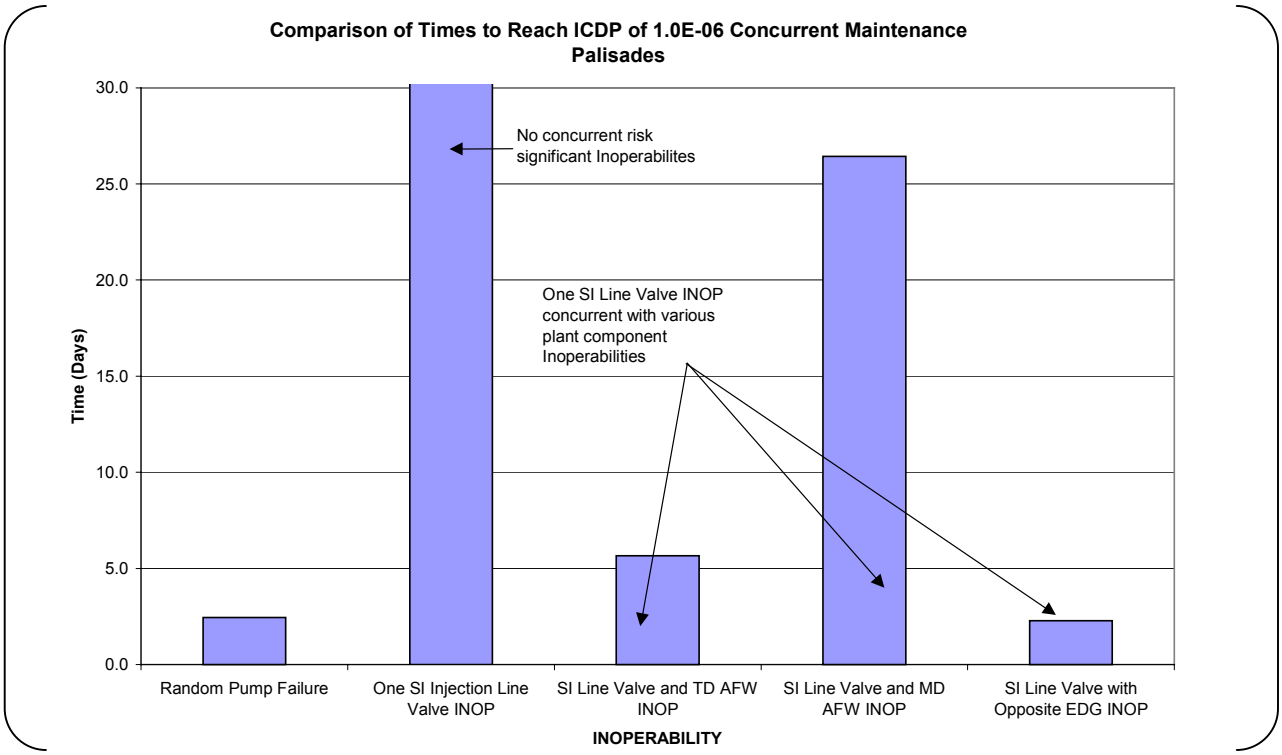


Figure 6.3-10

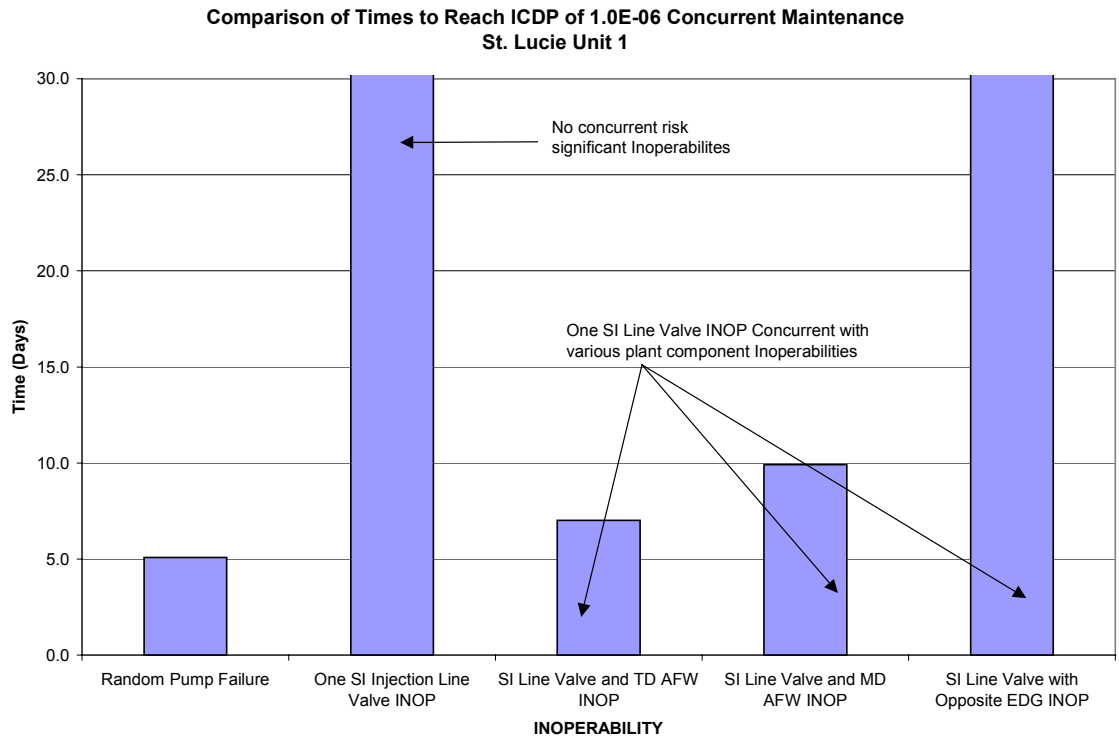


Figure 6.3-11

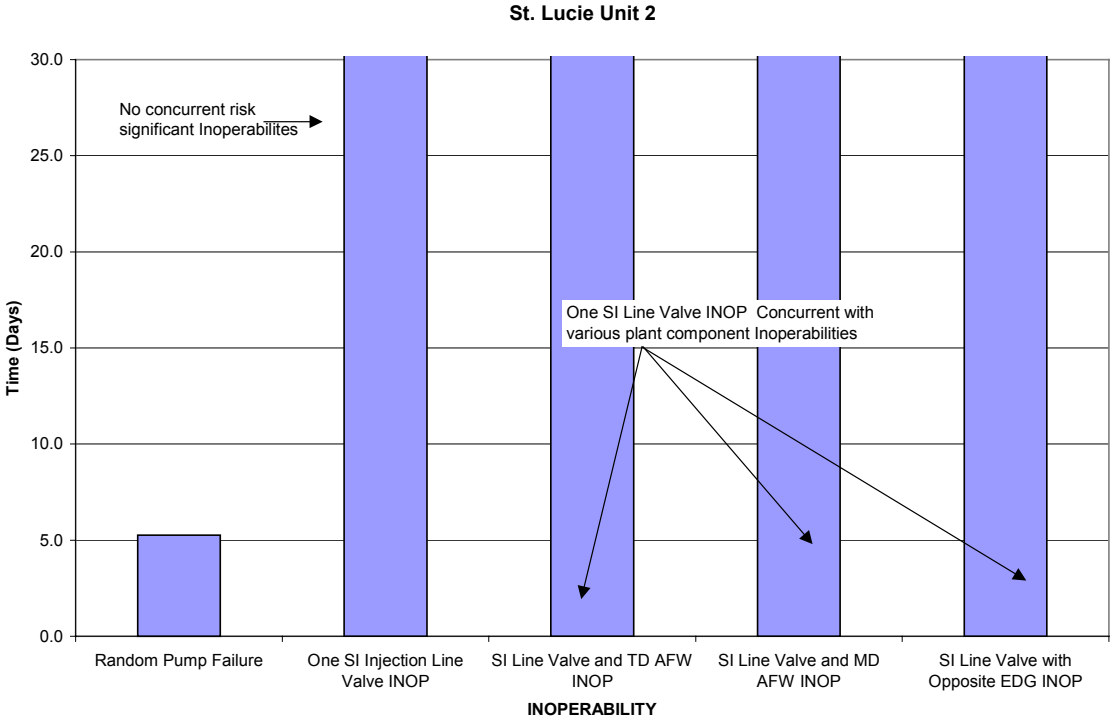


Figure 6.3-12

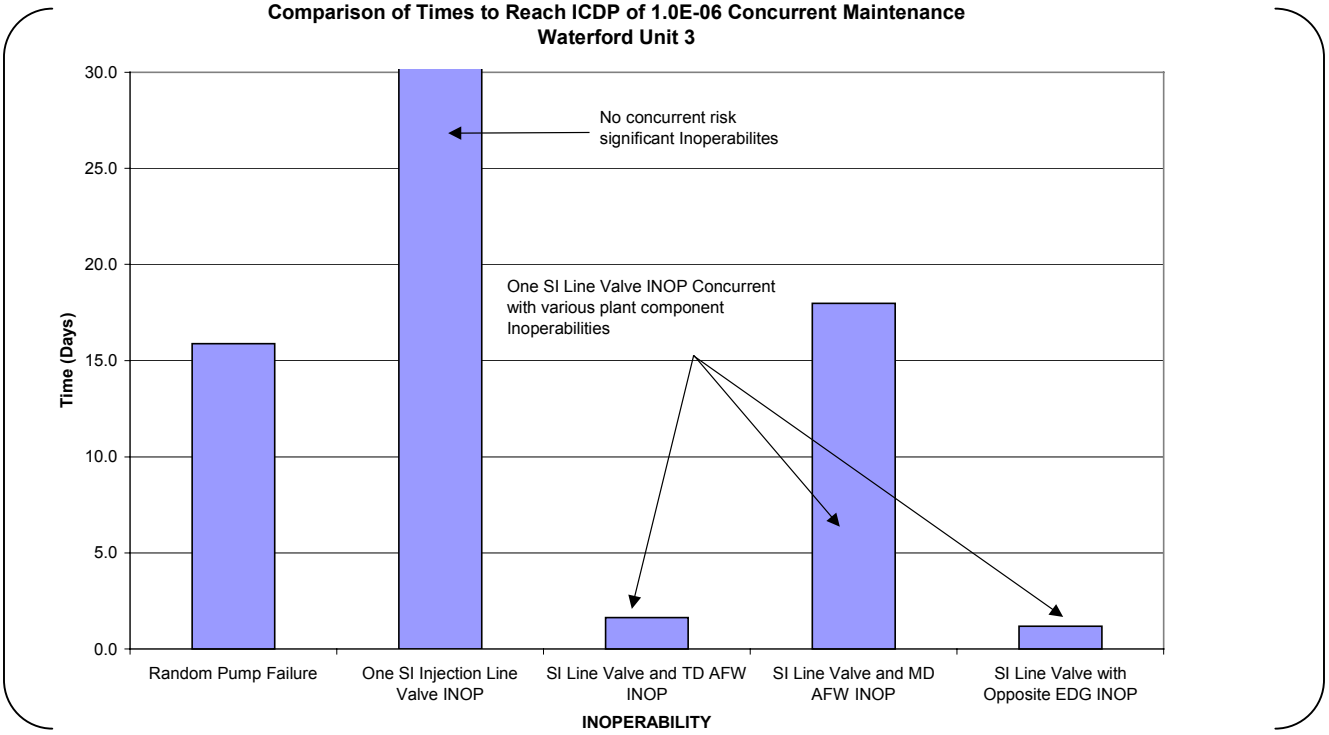


Figure 6.3-13

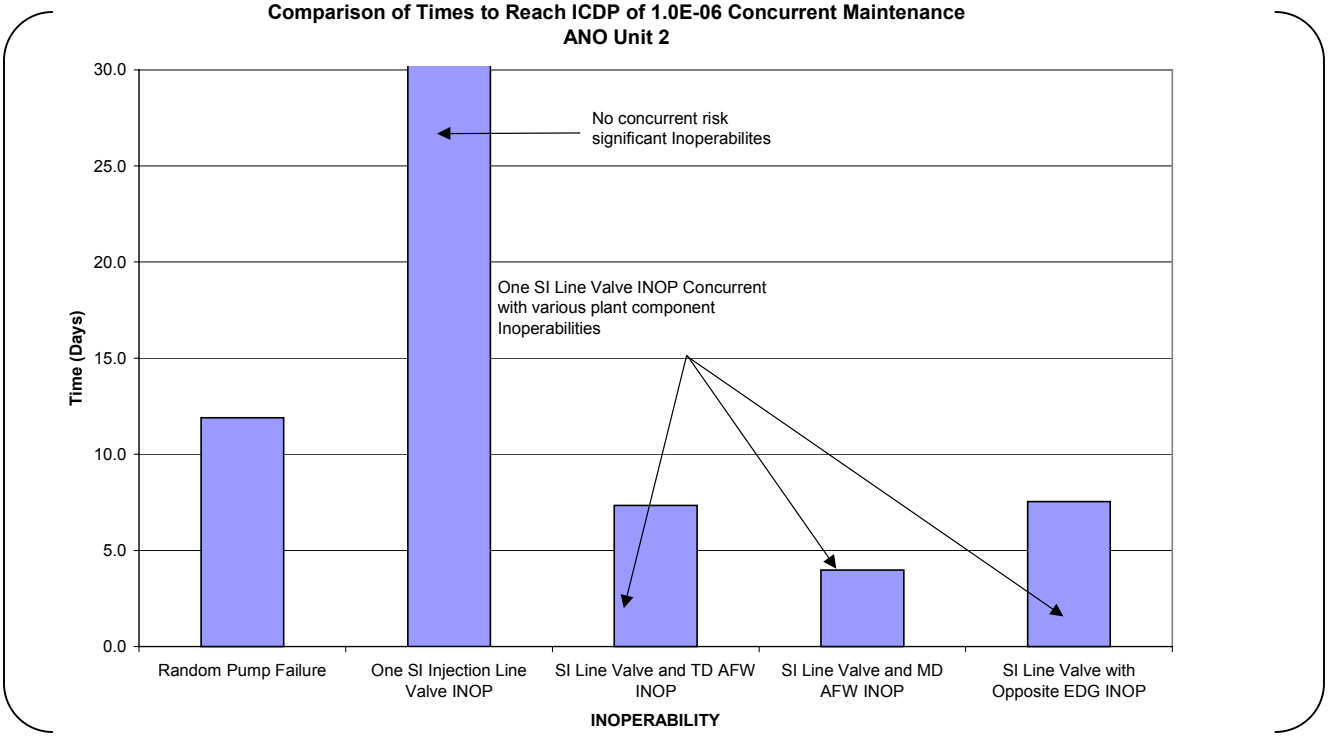


Figure 6.3-14

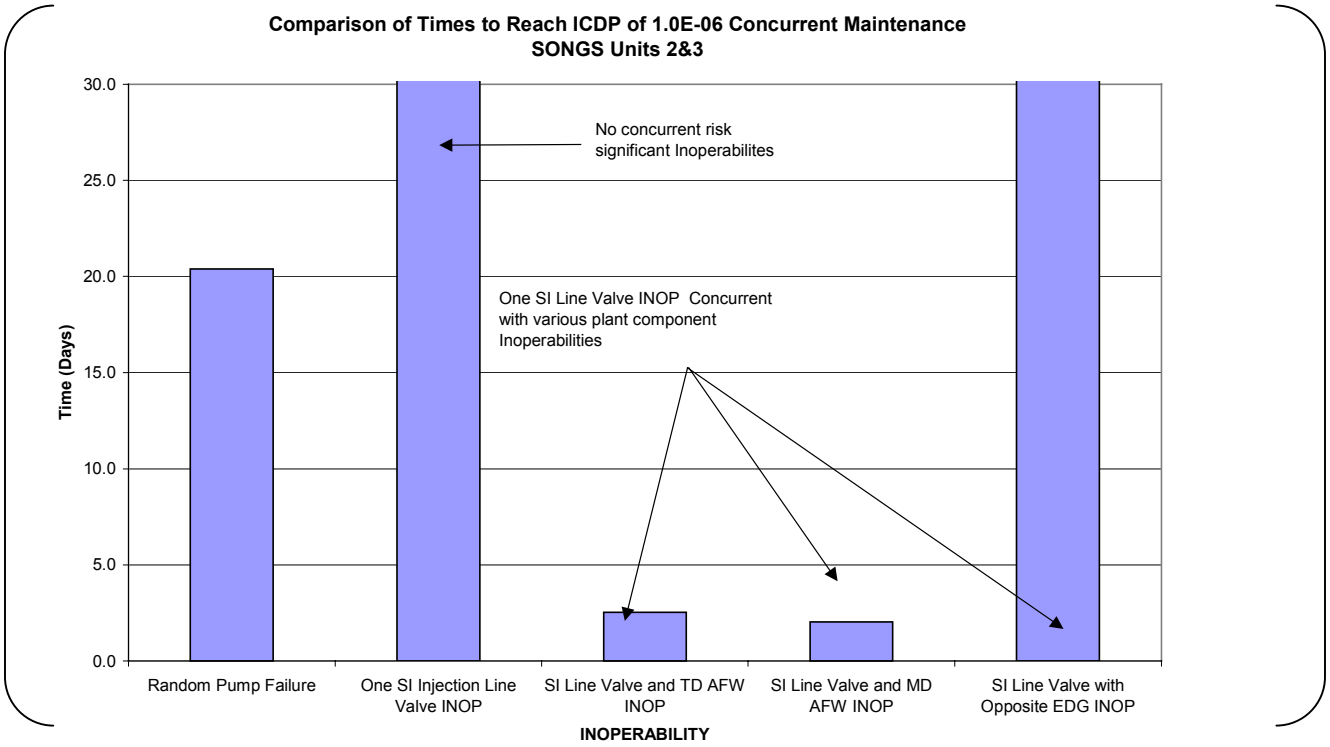


Figure 6.3-15

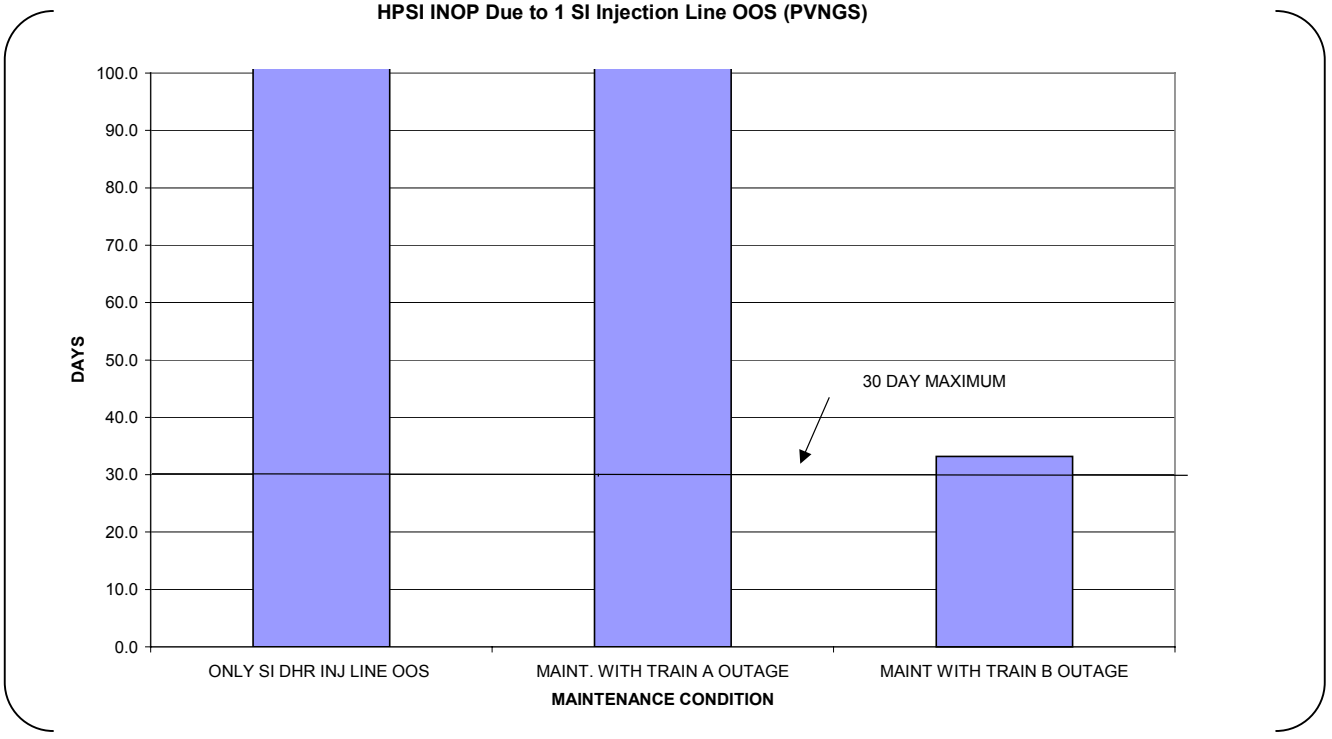
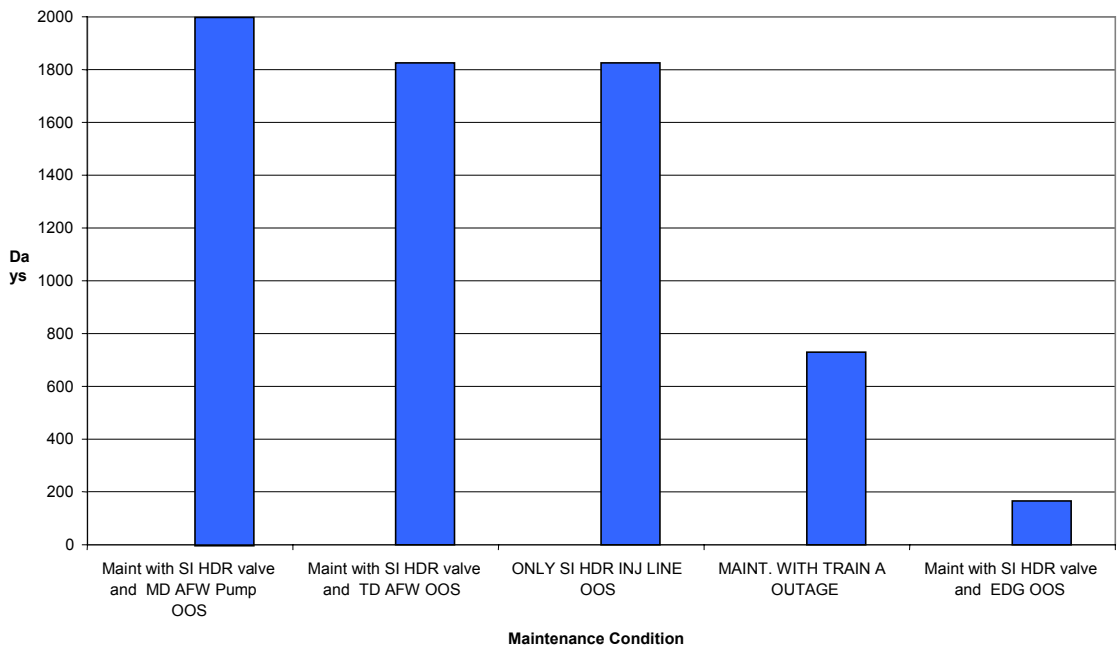


Figure 6.3-16



6.3.2.6 Fire and External Events

6.3.2.6.1 Fire Risks

A review of CEOG member plant CDFs indicates that the overall contribution from external events (including seismic and fire) varies from between 0.1 to twice the plants internal events CDFs. Fire results vary according to plant design and level of conservatism in the modeling. For the CEOG member plants, fire CDFs vary from 6.0E-06 per year to 5.8E-05 per year. For the most part, fire CDFs are overly conservative as many plants establish the fire CDF based on the EPRI "FIVE" methodology (Reference 25). While present values are upwardly biased, these evaluations provide important insights associated with the importance of equipment required for safe shutdown. A detailed study of the incremental effect of fire associated with HPSI maintenance was performed for PVNGS, a representative later generation CE designed PWR. The results of that study are reported in Table 6.3-6. The PVNGS analysis includes a detailed fire risk PSA. As discussed previously, the PVNGS unit (as well as San Onofre Nuclear Generating Station (SONGS) Units 2 and 3 and Waterford-3) have no PORVs and cannot use the HPSI system for feed and bleed. Based on these results, HPSI train OOS risk is not expected to impact fire induced core damage results. The primary risk impacts of fire are associated with equipment used to mitigate related scenarios (e.g. EDGs, AFW, etc.) as unavailability of these components degrades safe shutdown pathways. Availability of safe shutdown paths will avoid RCS inventory loss and hence obviate the need for HPSI mitigation during and following a fire. Consequently, the risk impact of HPSI system unavailability on fire CDF is small.

Table 6.3-6
Example Incremental Fire Risks for PVNGS

HPSI Inoperability	Concurrent Equipment OOS	Incremental Fire CDF (per day)
Any	Random Unavailability	< 2.0E-10
SI Room Cooling	Complete HVAC Train	< 7.0E-08
SI Injection Valve	EDG	< 2.0E-08
SI Injection Valve	MD AFW Pump	< 1.0E-07
SI Injection Valve	TD AFW Pump	< 1.1E-07
SI Injection Valve	Train A or B Maintenance Week	Negligible

6.3.2.6.2 Seismic Risks

Seismic risk contributions are plant specific. Plants sited in low seismic regions have negligible seismic impact while the seismic contribution to core damage at SONGS is about 50% of the internal events risks. Plant with larger seismic risks typically include consideration of the dominant seismic risks in their risk assessment process. The unavailability of a HPSI train will pose a small impact on seismic risk as the HPSI system may be needed to mitigate seismic induced LOCAs and LOCA events resulting from stuck open PORVs/PSVs. However, due to the low fragility of RCS piping and the low frequency of a large seismic event, seismic induced LOCA frequencies are low. Furthermore, seismic events that fail one HPSI train would likely fail both, and that the significance of the HPSI for mitigation is limited. Based on the preceding, the HPSI system is expected to have overlap with risk.

An example quantitative seismic risk impact assessment was performed using the SCE PSA. In this assessment the impact of a complete non-functionability of a HPSI train was evaluated for its impact on the plant's seismic PSA. The study indicated that the unavailability of a HPSI train would increase seismic risk by 1.22E-06 per year (about a 15% increase in the seismic risk). The incremental seismic risk for a 30 day AOT exposure will be less than 1.0E-07. Thus, the impact of lesser degradations is very small and should not impact risk-informed decision making with respect to HPSI system and related inoperabilities.

As the seismically induced LOCA initiating event frequency is small (~ 1.0E-06 to 1.0E-07 per year), the demands on mitigating equipment will be low and the likelihood that mitigation equipment would not survive a seismic event sufficient to cause a LOCA is expected to be large. For other initiators, provided safe shutdown paths are protected for any PWR, the presence or absence of the HPSI will not have a significant impact on plant risk.

6.3.2.7 "At Power" Analyses Conclusions

Analyses presented in Section 6.3.2.3 demonstrate that analytical techniques are capable of modeling risks associated with the HPSI train inoperabilities, both alone and in conjunction with other system equipment outages. Results of these analyses indicate that many HPSI train inoperabilities have a small impact on plant risk and may be candidates for extended maintenance, as appropriate.

6.3.3 Assessment of Transition Risk

For any given AOT extension, there is an associated "at power" increase in risk. This increase may be negligible or significant. A complete approach to assessing the change in risk also accounts for the effects of avoided shutdown, or "transition risk." Transition risk represents the risk associated with changing the operating mode of a Light Water Reactor from its nominal full power operating state to a lower shutdown mode following equipment failure, in this case, one HPSI train being inoperable. Transition risk is of interest in understanding the tradeoff between shutting down the plant and restoring the HPSI train to operability while the plant continues to operate. In accordance with the Maintenance Rule risk assessment guidance (Reference 2), the risk of transitioning from "at power" to a shutdown mode may be balanced against the risk of continued operation and performing corrective maintenance while the plant is at power. Two risk analyses were considered. In one assessment the risk of transitioning from Mode 1 to Mode 3 was established without assuming inoperability of any risk significant equipment. The second analysis assumed that a HPSI train was inoperable transitioning from Mode 1 to Mode 3. Results of representative transition risk assessment for various CE designed PWRs suggests that transition risks varies from 1.0E-07 to greater than 3.0E-06. Transition risks depended upon main and auxiliary feedwater system design and reliability, and the significance of unavailable equipment. The results of transition risk presented in Table 6.3-7 are illustrative only. However, it is reasonable to assume that provided incremental “at power” operational risks are small (less than 1.0E-06), continued power operation will largely be offset by avoidance of a plant transition. Additional details of this analysis are available in References 17a and 21.

Table 6.3-7
Estimated Transition Risks (ΔCDP) for Representative CE Designed PWRs

Plant	Transition Risk Contribution (One CSS Train Unavailable, Reference 17a) (1)	Transition Risk Contribution (One HPSI Train non-functional, Reference 21)
Fort Calhoun	1.06E-07	1.38E-06
Millstone, Unit 2	NA	2.44E-06
WSES, Unit 3	NA	2.53E-07
San Onofre, Units 2 & 3	1.64E-06	3.2E-06
Arkansas Nuclear One, Unit 2	NA	NA
St. Lucie Units 1 & 2	NA	NA
Palo Verde 1, 2 & 3	3.24E-06	3.2E-06

Notes:

(1) One CS train Not available. This represents a minimal risk transition for CE designed PWRs that have redundant and diverse containment heat removal systems.

NA - Not Available

6.3.4 Assessment of Change in Large Early Release Frequency (LERF)

A review of large early release scenarios for the CE designed PWRs indicates that early releases arise as a result of one of the following three classes of scenarios:

1. Containment Bypass Events

   These events include interfacing system LOCAs and steam generator tube ruptures (SGTRs) with a concomitant loss of SG isolation (e.g., stuck open Main Steam Safety Valve (MSSV)).

2. Severe Accidents accompanied by loss of containment isolation.

   These events include any severe accident in conjunction with an initially unisolated containment.

3. Containment Failure associated with energetic events in the Containment.

   Events causing containment failure include those associated with the high pressure melt ejection phenomena (including direct containment heating) and hydrogen conflagrations/detonations.

Of the three release classes, Class 1 tends to represent a large early release with potentially direct, unscrubbed fission products to the environment. Class 2 events encompass a range of releases varying from early to late releases that may or may not be scrubbed. Class 3 events result in a high pressure failure of the containment, typically immediately upon or slightly after reactor vessel failure. Detailed Level 2 analyses for the plant condition with one inoperable HPSI train were not performed. These events are typical of the LERF events defined in Reference 26. Assessment of the expected change in the large early release fraction was made by assessing the impact of the unavailability of the HPSI System on the above event categories.

A review of event classes suggests that the impact of an incremental core damage risk of 1.0E-06 will result in a conditional early containment failure probability of less than 0.10, as the HPSI system is primarily required for intermediate and low pressure sequences. Bounding LERF analyses for complete HPSI train unavailability performed in support of an extended time for system inoperabilities (Reference 21, Table 4.2-1) indicated a LERF contribution of 1.6E-9 per hour with an associated CDF of 2.7E-07 per hour. This resulted in a conditional LERF factor of 1.6E-9/2.7E-7 (or 0.006). Thus, a HPSI unavailability resulting in a 1.0E-06 ICDP would result in an ILERP of 6.0E-09. This LERP increment is very small. Regardless, consistent with the Maintenance Rule, plant entry into the AOT/CT will consider configuration specific LERF implications of the HPSI maintenance.

6.3.5 Risk Assessment Summary

The proposed application of a flexible AOT for HPSI was evaluated from the perspective of various train inoperabilities. Incorporation of the flexible AOT into the technical specification is expected to result in negligible to small increases in the "at power" risk consistent with RG 1.174 and NUMARC 93-01. Risks of plant operation within the backstop AOT will vary depending upon the HPSI component in maintenance, concurrent equipment outages, and plant administrative control processes (See Appendix B). For example, increases in risk associated with PM on many HPSI system MOVs at power are negligible. Small risk increases are possible when more risk significant components of a HPSI train are OOS. However, preventive maintenance on components that will render the system non-functional is expected to be a far less frequent event and will typically consume much less time than that afforded by the maximum 30 day backstop AOT.

Assessment of large early release probabilities concluded that increased unavailability of the HPSI system will result in a negligible impact on the large early release probability for CE designed PWRs.

The flexible AOT will also allow the plant to respond to system failures while remaining at power. The significance of these failures within the HPSI system will vary. Provided the component failure does not underlie a similar failure in the redundant HPSI train, the risk associated with the repair can be assessed and managed such that the accumulated “at power” risk will be small. During the current and extended timeframes of the AOT, plant risks will be managed consistent with 10 CFR 50.65. When risks are sufficiently large, the extended AOT risks will be tracked in order to confirm that the risk associated with implementing the RMTS is acceptable.

6.4 RISK INSIGHTS/COMPENSATORY MEASURES

As part of implementing the Maintenance Rule, each CE designed PWR utility has developed a method for configuration control during maintenance. Those methods are in compliance with 10 CFR 50.65(a)(4). An enhanced version of these procedures has been developed to describe HPSI RMTS guidance (See Appendix B). The information presented should allow the flexible AOT applicability to be globally expanded to other appropriate equipment TS. The impact on risk is evaluated prior to removing the equipment from service for cases where a planned maintenance or other activity is to be performed on a system/train concurrent with other maintenance.

The risk associated with any particular maintenance evaluation will be performed in accordance with the Maintenance Rule. Once within the extended portion of the AOT, the cumulative incremental risk of the flexible AOT will be estimated and tracked. This tracking will supplement the maintenance rule aggregate risk assessment and confirm that the annual incremental risk associated with implementation of the RMTS concept is small per RG 1.174.

Corrective maintenance on a HPSI train "at power" can be justified on the basis that the plant risk increment is small, and that maintenance at power reduces the overall plant risk by avoiding

an unnecessary plant mode transition. However, in drawing this conclusion the current risk status of plant equipment at the time of the HPSI train unavailability, including the impact of other OOS equipment, must be considered.

The HPSI system plays an important role in managing plant risk. If a HPSI train is declared inoperable and the repair, surveillance, etc. will potentially exceed the frontstop AOT/CT, the plant staff will manage the risk and define compensatory measures, as appropriate. Risk insights suggest typical administrative actions that may be taken during "at power" include the following:

1. For many CE designed PWRs, the HPSI system may be used for Once-Through-Core-Cooling and therefore can backup the AFW in satisfying the RCS heat removal safety function. For this class of plants, concurrent maintenance on the HPSI and AFW systems (and other support feedwater systems) should be carefully controlled. This risk insight applies to all operating modes where the steam generator is used for heat removal. This guidance will be captured in plant administrative controls.

2. Critically evaluate requests for concurrent system maintenance, and minimize concurrent maintenance even in the inoperable train. While this is not a requirement, the plant using RMTSs should consider providing guidance to limit risk by unnecessarily rendering an entire system non-functional as a result of a declared system inoperability that retains significant HPSI function. The current TS AOT does not allow maintenance of both trains (i.e. entire system). A declared inoperable system may be generally functional. For example, maintenance of a single HPSI injection valve would have negligible impact on the functionability of the overall HPSI system. However, simultaneous maintenance on multiple valves could fully disable the affected HPSI train. Therefore, a series of maintenance states with partial equipment inoperabilities may result in significantly lower accumulated risks.

3. In a corrective maintenance situation, the potential for the failure mechanism to similarly impact redundant components in another train should be assessed. This effort should be performed early in the repair process as practical and may include risk analyses or testing of redundant equipment. Typically, the plant corrective action programs will resolve the issue expeditiously. In any event, the CDF potential must be resolved and/or considered prior to exiting of the frontstop AOT/CT and entering into the extended portion of the AOT/CT.

4. Prior to entry into the extended portion of the AOT/CT risk management actions should consider, as appropriate, utilization of non-safety equipment and/or temporary procedures to control risks. These actions could consider procedures to return the affected HPSI train to functional use, if not full operability, if the need arises. For example, for failure of one HPSI HVAC cooling train, methods should be defined for establishing temporary cooling, should the need arise. The extended degree to which risk management actions are implemented will be dependent on the risks of the extended outage and the efficiency of associated actions. Risk management actions that have been formally implemented and reviewed via the plant PSA and operations staff may be credited in the extended AOT/CT PSA assessment.

Enhanced high level guidance for compliance with the Maintenance Rule (a)(4) is summarized in Appendix B.

6.5 COMMENT ON DEFENSE-IN-DEPTH

The proposed change to the technical specification applies to extending the allowed time for inoperabilities of a single HPSI train. In accordance with the philosophy for permitting limited duration inoperability of equipment, the available redundant HPSI train provides adequate defense-in-depth during the period when one HPSI train is inoperable. Additional guidance to critically evaluate simultaneous outages of the AFW and HPSI trains further enhances defense-in-depth by ensuring the potential challenges to core cooling are adequately controlled.

This page intentionally blank.

7.0 PROPOSED MODIFICATIONS TO NUREG-1432

Appendix A includes proposed changes to the following sections of NUREG-1432, Revision 02, Reference (9):

a. 3.5.2, ECCS - Operating
b. B 3.5.2, ECCS - Operating

The TS modification incorporates an option to implement alternative actions to allow additional time to repair (or otherwise resolve) a TS inoperability beyond the 72 hours Completion Time. The proposed RMTS is also presented in Table 6.1-1. The proposed ISTS changes are summarized in Appendix A. The proposed changes associated with the flexible AOT/CT are discussed below.

B.1 Restore inoperable HPSI Train to Operable Status (Completion time 72 hours)

If one HPSI train is inoperable, it must be restored to OPERABLE status within the frontstop AOT (72 hours). The components in this degraded condition are capable of providing 100% of the ECCS flow requirements following an accident. The frontstop AOT/CT was developed taking into account the redundant capabilities afforded by the OPERABLE train and the low probability of a DBA occurring during this period.

Note: This action is analogous to the current HPSI train requirement. In accordance with the Maintenance Rule (10 CFR 50.65(a)(4)), a risk assessment will be performed prior to a planned removal of equipment from service. However, upon entry into this TS for any reason, the plant personnel will confirm that an existing evaluation is applicable or that the entry is for the purpose of unplanned corrective maintenance and perform a risk assessment of the plant configuration in a manner consistent with 10 CFR 50.65(a)(4) following the associated guidance set forth in NUMARC 93-01 Rev 03, Section 11, for quantitative and/or blended risk assessment approaches. This activity is consistent with the implementation of the Maintenance Rule at CE designed PWRs. In accordance with the plant corrective action program, assessment of common cause failure potential will be performed. If repair of the inoperable HPSI train cannot be completed within the required AOT/CT, Actions B.2.1 and B.2.3 must be performed.

Required Actions B.2.1 through B.2.3

A risk evaluation must be performed prior to the expiration of the frontstop AOT which demonstrates the acceptability of a Completion Time extension after the expiration of the frontstop AOT completion time (e.g. 72 hours) for this configuration. Additional risk evaluations are performed whenever configuration changes that affect the plant risk occur to determine if the plant configuration (considering this degraded condition and any other degraded conditions) is acceptable for continued operation beyond the frontstop. If at any time after the expiration of the frontstop it is determined that the level of plant risk created by the degraded plant configuration is not acceptable for continued operation, this Required Action and associated Completion Time are not met. The factors considered in establishing the risks of the HPSI inoperability are shown in Action B.2.1. Regardless of the risk, the inoperable equipment

or level of degradation causing entry into this Condition must be restored to OPERABLE status or compliance with the LCO must be met prior to the Completion Time reaching the 30 day backstop limit. If this has not occurred, the Required Action and associated Completion Times are not met.

Action B.2.1 Completion Time Extension beyond 72 hours (Completion time 72 hours)

A risk assessment justifying continued power operation must be performed prior to extending the repair time for the HPSI train, beyond the CT of required new Action B.1. The assessment will consider the risk impact of extending the repair with consideration of the following factors:

1. Potential for common cause coupling,

2. Risk of the extended completion time based on the contemporaneous plant configuration (including consideration of non-internal contributors),

3. Time required to complete repair,

4. Risk impact of contingency actions, and

5. Potential risks associated with shutdown and transition.

As a target, repairs that will result in net incremental CDP of less than 1.0E-06 and LERP of less than 1.0E-07 may be undertaken with minimal implementation of risk management actions. Higher risk evolutions may involve implementation of contingency actions and may also be undertaken provided the absolute plant risks are small (consistent with Maintenance Rule Guidance). An assessment of risk and implementation of risk management actions should accompany higher risk evaluations when the overall maintenance risk requires extra-normal work controls (See Reference 2). It should be noted that prior to entering the extended AOT/CT, the common cause potential of the failure should be resolved or appropriately considered in the risk assessment. In accordance with NUMARC 93-01, risk assessments should also consider (either quantitatively or qualitatively) the impact of relevant external events.

Assessments made to support entry into the extended AOT/CT should be documented.

Action B.2.2 Determine that the Risk Configuration is Acceptable for Continued Operation beyond 72 hours (to be performed whenever configuration changes which may affect the plant risk occur).

In this step the plant will monitor risk changes in the plant as impacted by the removal of equipment from service. In this case of the HPSI system, operation in this region would impact system performance indicators, and would therefore be subject to review within the context of the of the reactor oversight process.

The risk evaluation should consider the contemporaneous plant configuration time required to complete repair, impact of contingency actions and risks associated with transition and

shutdown. Risk significant plant state changes should be evaluated within 24 hours. Acceptable plant risks are determined based on Maintenance Rule processes.

The Maintenance Rule is concerned with managing the risks associated with maintenance and equipment outages. As the risk profile of the plant changes the plant will reassess the impact of the extended inoperability to assess a need for a change in plant operations and take appropriate actions to control risks. The guidance is expected to be risk-informed, as in certain instances the plant activity should emphasize return of high risk components to service as quickly as possible. The risk impact of the inoperability will be reflected in reconsideration of contingency actions, and the efficiency of the shutdown action. Risk assessments and/or other evaluations (both qualitative and quantitative) contributing to decisions to enter and remain in the extended CT will also be documented. When no plant state change occurs in the time interval since the previous evaluation, a new evaluation is unnecessary.

Action B.2.3 Restore train to Operable status [Acceptable Completion Time Extension CT or 30 days, whichever is less]

This action requires the inoperable HPSI train be returned to operable status prior to incurring unacceptable risk. Plant risks will be controlled via Maintenance Rule processes with consideration of plant shutdown, contingency actions and time required to complete repair. Regardless, the HPSI train must be returned to operable status within 30 days. The 30 day backstop ensures that the plant is returned to be in compliance with its design basis.

Additional Comments RMTS Implementation: Interface with other Regulations (RG 1.174)

Note, it is not the intention for the risk contribution of the RMTS to cause a significant yearly increase in CDF. The Maintenance Rule programs are reviewed to ensure plant risks are properly managed and that the plant CDF does not increase significantly. Incremental annual risk associated with the RMTS will be controlled to fall within Region II or Region III of the NRC acceptance guidelines (Figures 3 and 4 of Reference 3a). Furthermore, the overall goal in any given year is less than 10% change in plant CDF due to the TS change. For most PWRs, associated CDF increases will be on the order of 1.0E-06 to 4.0E-06 in any given year. Entries into the extended AOT are expected to be controlled so that the yearly risk increment will be small. Risks at this level will be offset largely by avoidance of mode transitions risks.

CEOG process perspectives on the implementation of the flexible AOT are presented in Appendix B. Specifically, implementation of the flexible AOT/CT for CEOG designed PWRs will include the following:

1. A risk-informed assessment of the contemporaneous plant configuration. The assessment would require, as a minimum, a quantitative assessment using a level one internal events PSA. Qualitative assessments should be performed where appropriate to enhance quantitative evaluations or to assess the overall risk when quantitative tools are available. As discussed previously, HPSI subsystem inoperabilities are expected to have a negligible impact on LERF. Therefore, LERF need only be assessed during periods of

equipment inoperabilities that are important to LERF that may be OOS during the HPSI extended AOT/CT period.

2. All elements of the level one PSA must meet the minimum attributes for a risk-informed application when evaluated by a peer review team in accordance with NEI 00-02, industry peer review guidance document, or "conditional" grades must be resolved, or the impact of those elements not meeting the requirements should be demonstrated to not be risk significant as it applies to the use of the flexible AOT/CT.

3. The PSA should be current and it should be evaluated for update (model update and data update) on a minimum interval of two refueling cycles. When no update is performed a demonstration that such an update is not required should be provided. Modifications to the plant resulting in non-minimal risk effects (changes to baseline risk, or changes to distribution of significant equipment or actions) must be reflected in the PSA, or otherwise accommodated in the risk assessment process, in a timely manner.

4. The risk-informed decisionmaking process should have the capability to contemporaneously model the plant configuration, and determine the configuration-specific CDF and LERF in a time frame consistent with the expected plant risks. That is, it should be capable of addressing emergent conditions in a timely manner.

5. The assessment must consider instantaneous risk, integrated risk for a given configuration, and aggregate risk as discussed in NUMARC 93-01. The quantitative guidelines for each of these parameters are specified in NUMARC 93-01.

6. Explicit risk management actions (e.g., Mode Change, including shutdown and compensatory measures) based on the above quantitative guidelines, and other qualitative PSA and risk insights, may be developed and documented in advance for anticipated combinations of equipment with more significant risk impacts.

7. The assessment, results, and associated risk management actions must be documented and available for subsequent NRC audit or inspection.

Whenever plant operation with an extended AOT/CT maintenance condition exceeds the nominal CDF/LERF for "normal" maintenance, the extended AOT/CT will be tracked. Tracking of the incremental annual risk impact of the RMTS will be performed. Incremental risk increase may be considered in conjunction with the impact of contingency actions and shutdown/ transition alternatives. A summary of the impact of tracked Incremental Conditional Core Damage Probability and Incremental Conditional Large Early Release Probability will be documented and used for self evaluation of the use of the RMTSs and the plant success in meeting RG 1.174 guidance. Results of the review will be factored into the plant's corrective action program, as appropriate.

The actual TS change is likely to result in plant maintenance changes to allow use of larger fractions of existing completion times. In many instances, plant maintenance protocols avoid planning activities greater than one-half of the completion times. As a result, longer duration

maintenance activities are often subdivided into more than one step so that they are performed on multiple entries. This creates inefficiencies and actually prolongs component declared inoperability, therefore increasing plant risk. Furthermore, flexibility to utilize longer AOTs/CTs can potentially avoid higher risk system outages which result from situations that drive the plant to complete more comprehensive maintenance activities to minimize system outage times and meet performance goals.

This page intentionally blank.

8.0 SUMMARY AND CONCLUSIONS

This report provides the results of an evaluation to modify TS 3.5.2 to a risk-informed alternative, which allows consideration of extending a low risk inoperability of a single HPSI train beyond the frontstop or existing AOT/CT. This AOT extension is sought to provide needed flexibility in the performance of both corrective and preventive maintenance during power operation. Justification of this request is based on an integrated review and assessment of plant operations, deterministic/design basis factors and plant risk. Results of this study demonstrate that the proposed TS changes provide plant operational flexibility while simultaneously allowing continued plant operation with an acceptable level of risk.

The plant risk will be managed via the Maintenance Rule and associated processes. For the plants evaluated, incorporation of the proposed TS would result in negligible to small increases in the "at power" risk. Furthermore, overall maintenance risks will be tracked via the Maintenance Rule and/or Reactor Oversight Process. The utilization of the flexible AOT/CT is specifically tracked and compared annually to the RG 1.174 ΔCDF and ΔLERF maps to ensure that the RMTS has not resulted in a significant risk increase.

The unavailability of one train of HPSI does not significantly impact events that result in a large early radionuclide releases. Therefore, any decrease in availability of the HPSI System would result in only a negligible impact on the large early release probability for CE designed PWRs.

This page intentionally blank.

9.0 REFERENCES

1. 10 CFR 50.65, Appendix A, “Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," NRC, July 19, 1999 (64FR38551)

2. NUMARC-93-01, Revision 3, “NEI Guidelines for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants,” NEI, July 2000.

3a. RG 1.174, “An Approach for using Probabilistic Risk Assessment in Risk Informed Decisionmaking on Plant Specific Changes to the Licensing Basis,” USNRC, July 1998.

3b. RG 1.177, “An Approach for Risk Informed Decisionmaking: Technical Specifications,” USNRC, August 1998.

4. “Risk Informed Technical Specification: Project Description,” NEI, June 2001.

5. TSTF 358, Revision 6, “Missed Surveillance Requirements,” September 2001.

6. TSTF 359, Revision 6, “Increase Flexibility in Mode Restraints,” October 8, 2001.

7. LER #94-005-01, Palo Verde Unit 2.

8. NUREG-0212, Revision 3, "Standard Technical Specifications for Combustion Engineering Pressurized Water Reactors," July 9, 1982.

9. NUREG-1432, Revision 02, "Standard Technical Specifications: Combustion Engineering Plants," April 2001.

10. CE-NPSD-593, “Partial Response to NRC Generic Letter 89-19: Small Break LOCA Recovery with Low Head HPSI,” CEOG Task 651, CE Owners’ Group, October 1990.

11. Maine Yankee, Individual Plant Examination, Volume 1, YAEC 1992.

12. 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear reactors," January 1, 1991.

13a. CEN-114-P, "Review of Small Break Transients in Combustion Engineering NSSSs," Combustion Engineering, Inc., July, 1979.

13b. CEN-152, “Emergency Operating Guidance,” Combustion Engineering, Inc.

14. NUREG 0800, Revision 2, USNRC Standard Review Plan, July 1981.

15. TID 14844, "Calculation of Distance Factors for Power Reactor Sites," USAEC, 1962.

16a. Fort Calhoun Station, Individual Plant Examination, Omaha Public Power District, December, 1993.

16b. RAN-92-006, Revision, "Calvert Cliffs Nuclear Power Plant, BG&E, December 1992.

16c. Millstone Unit 2 Individual Plant Examination, Northeast Utilities, December 1993.

16d. St. Lucie Units 1&2, Individual Plant Examination, St. Lucie Nuclear Generating Station December 1993.

16e. ANO2 Individual Plant Examination, Arkansas Power & Light, August 1992.

16f. Waterford Unit 3, Individual Plant Examination, LP&L, August 1992.

16g. San Onofre Units 2 & 3, Individual Plant Examination, SCE, April 1993.

16h. Palo Verde Nuclear Generating Units 1, 2 & 3, Individual Plant Examination, Arizona Public Service, April 1992.

17a. CENPSD-1045-A, "Joint Application Report: Modifications to Containment Spray System Technical Specifications," CE Owners' Group, March 1998.

17b. CE-NPSD-996, "Joint Applications Report: Emergency Diesel Generator AOT Extensions," CE Owners' Group, June 1995.

17c. CE-NPSD-1168-A, Revision 00, "Joint Applications Report for Containment Isolation Valve AOT Extension," CE Owner's Group, January 2001.

17d. CE-NPSD-1184-A, Revision 00, " Joint Application Report for DC Power Source Allowed Outage Time Extension," CEOG, May 2001.

18. INEEL/EXT-99-00373, "High Pressure Safety Injection System Reliability: 1987-1997," INEL, Poloski, et.al., July 1999.

19. NUREG/SR-1649, Revision 3, "NRC: Reactor Oversight Process," USNRC, May 3, 2002.

20. NUREG/CR-5750, "Rates of Initiating Event at US Nuclear Power Plants," 1987-1995, INEEL, February 1999 (Appendix J).

21. CE-NPSD-1041-P, "High Pressure Safety Injection System Technical Specification Modifications," ABB Inc., September 1996.

22. CEN420-P, Small Break LOCA Realistic Evaluation Model, November 1993, Combustion Engineering, Inc.

23. NEI-99-002, “Probabilistic Risk Assessment Peer Review Process Guidelines,” NEI, April 2000.

24. Letter, Baev, R.L. to Stello, V., “Recommended Interim Revisions to LCO’s for ECCS Components,” NRC, December 1, 1975.

25. TR-100370, “EPRI Fire Induced Vulnerability Evaluation (FIVE),” EPRI, April 1992.

26. NUREG-CR6595, BNL-NUREG-52539, “An Approach for Estimating the Frequencies of Various Containment Failure Modes and Bypass Events,” Sandia National Laboratory, Prath, W., et.al., January 1999.

This page intentionally blank.

Appendix A

"Mark-up" of NUREG-1432 Tech Specs 3.5.2 & Bases (ECCS – Operating)

and

Tech Spec 5.5 (Programs and Manuals)

Existing Action Statement for LCO 3.5.2

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
- REVIEWER'S NOTE The adoption of this Condition is contingent upon implementation of a program to perform a contemporaneous assessment of the overall impact on safety of proposed plant configurations prior to performing and during performance of maintenance activities that remove equipment from service.			
A. One LPSI subsystem inoperable.	A.1	Restore subsystem to OPERABLE status.	7 days
B. One or more trains inoperable for reasons other than Condition A.	B.1	Restore train(s) to OPERABLE status.	72 hours
C. Required Action and associated Completion Time not met.	C.1	Be in MODE 3.	6 hours
	AND		
	C.2	Reduce pressurizer pressure to < [1700] psia.	12 hours
D. Less than 100% of the ECCS flow equivalent to a single OPERABLE train available.	D.1	Enter LCO 3.0.3.	Immediately

Delete the existing Condition B, Required Action B.1 and associated Completion Time with the proposed change (HPSI Risk Managed AOT/CT with a Backstop Example Format)

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
B. One HPSI train inoperable.	B.1	Restore inoperable HPSI train to OPERABLE status.	72 hours
		OR	
	B.2.1	Determine that the risk configuration is acceptable for completion time extension beyond 72 hours.	72 hours
		AND	
	B.2.2	Determine that the risk configuration is acceptable for continued operation beyond 72 hours.	Whenever configuration changes that affect plant risk occur
		AND	
	B.2.3	Restore inoperable HPSI train to OPERABLE status.	Acceptable completion time extension or 30 days, whichever is less.

Proposed Changes to the TS Bases are highlighted in **bold**. Existing References A1 through A6 of NUREG-1432 TS Bases 3.5.2 are supplemented with References A7 through A9.

ACTIONS

B.1, B.2.1, B.2.2, and B.2.3

If one or more trains are inoperable except for reasons other than Condition A (one LPSI subsystem inoperable) and at least 100% of the ECCS flow equivalent to a single OPERABLE ECCS train is available, the inoperable components must be returned to OPERABLE status within [72] hours**, or perform a risk-informed analysis to determine that the risk of continued operation in the current plant configuration is acceptable for extending the time of inoperability beyond [72] hours.** The 72 hour Completion Time is based on an NRC study (Reference A4) using a reliability evaluation **assuming one non-functional HPSI train** and is a reasonable amount of time to effect many repairs.

Required Action B.2.2 requires performing risk assessments as plant configuration changes during the HPSI train inoperability period. The inoperability of many TS components in conjunction with a single inoperable HPSI train may not be risk significant. However, the inoperability of an AFW train in conjunction with HPSI inoperability could have a significant impact on plant risk since many plants rely on HPSI as a RCS Heat Removal mechanism upon the loss of steam generator heat removal. Therefore, this action ensures that plant risks will continue to be assessed and appropriate action taken upon discovery of a risk-significant change in plant equipment configuration.

An ECCS train is inoperable if it is not capable of delivering the design flow to the RCS. The individual components are inoperable if they are not capable of performing their design function, or if supporting systems are not available.

The LCO requires the OPERABILITY of a number of independent subsystems. Due to the redundancy of trains and the diversity of subsystems, the inoperability of one component in a train does not render the ECCS incapable of performing its function. Neither does the inoperability of two different components, each in a different train, necessarily result in a loss of function for the ECCS. The intent of this Condition is to maintain a combination of OPERABLE equipment such that 100% of the ECCS flow equivalent to 100% of a single OPERABLE train remains available. This allows increased flexibility in plant operations when components in opposite trains are inoperable.

An event accompanied by a loss of offsite power and the failure of an Emergency Diesel Generator can disable one ECCS train until power is restored. A reliability analysis (Reference A4) has shown that the impact with one full ECCS train inoperable is sufficiently small to justify continued operation for 72 hours.

Depending on the plant configuration at the time of the HPSI component(s) inoperability, the risk of continued operation may be justified via a risk-informed analysis that follows guidance in accordance with 10 CFR 50.65(a)(4) (Reference A7) and consistent with NEI-93-01, Section 11, Revision 3 (Reference A8), as outlined in RG 1.182 (Reference A9). Extension of the Completion Time is based on acknowledgement that many HPSI system components are not risk-significant and that plants have adequate tools and controls in place for evaluating plant risks, implementing risk-informed actions and making appropriate risk-informed decisions. Regardless of the acceptability of the evaluated risk impact, the inoperable HPSI component(s) must be returned to OPERABLE status within the determined Completion Time up to a maximum of 30 days. This maximum limit provides sufficient time to complete repairs while taking into account HPSI system

operational goals and provides for return to a configuration as described in the deterministic accident analysis**.**

Reference A5 describes situations in which one component, such as a shutdown cooling total flow control valve, can disable both ECCS trains. With one or more components inoperable, such that 100% of the equivalent flow to a single OPERABLE ECCS train is not available, the facility is in a condition outside the accident analyses. Therefore, LCO 3.0.3 must be immediately entered.

Add to Tech Spec Section 5.5, "Programs and Manuals"

5.5.x Risk Management Program

This program details the processes utilized to evaluate plant risk and establish the appropriate risk management actions. This program uses 10 CFR 50.65(a)(4) guidance as a basis and expands it to include the plant specific risk practices and details the scope of the applicability of the program, plant specific PRA capabilities, and other risk insights.

REFERENCES

A1. 10 CFR 50, Appendix A, GDC 35.

A2. 10 CFR 50.46.

A3. FSAR, Chapter [6].

A4. NRC Memorandum to V. Stello, Jr., from R. L. Baer, "Recommended Interim Revisions LCOs for ECCS Components," December 1, 1975.

A5. IE Information Notice No. 87-01, January 6, 1987.

A6. CE-NPSD-995, "Low Pressure Safety Injection System AOT Extension," April 1995.

A7. 10 CFR 50.65(a)(4), "Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," 62 FR 59276, Nov. 3, 1997.

A8. NUMARC-93-01, Revision 3, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," Nuclear Energy Institute, July 2000.

A9. RG 1.182, "Assessing and Managing Risk before Maintenance Activities at Nuclear Power Plants," May 2000.

Appendix B

Risk Informed Processes for Implementing Risk Managed Technical Specifications

CEOG Perspectives

TABLE OF CONTENTS

B1.0 INTRODUCTION

10 CFR 50.36, "Technical Specifications," requires that the licensee identify minimum Limiting Conditions of Operation (LCOs). These are the minimum functional capability or performance levels of equipment required for safe operation of the facility. When an LCO is not met, the licensee shall shut down the reactor or follow any remedial action permitted by the Technical Specifications (TSs) until the condition can be met. No specific timing requirements were included in the regulation. However, in practice, actions within an LCO are associated with one or more fixed time intervals. Within the context of the plant TSs, these time intervals are termed the Allowed Outage Times (AOTs) or Completion Times (CTs). These time intervals were initially established at the time of plant licensing.

While simplified risk insights were considered in developing the AOTs/CTs, the values in the TSs for the most part are judgmental and reflect deterministic considerations. In the 1980s and early 1990s, risk-informed changes were approved for a number of plants including Millstone Units 2 and 3, Palo Verde Units 1, 2 and 3 and the South Texas Project. Early activities in integrating risk insights were used in resolving specific industry issues. These were sponsored to varying degrees by all Owner's Groups (References B1 and B2). In 1995, the NRC embarked on an initiative to improve regulatory efficiency and enhance public safety by considering risk insights in regulation. The effort resulted in the risk-informed changes to a wide range of regulatory activities including In-Service Testing (IST), In-Service Inspection (ISI), graded Quality Assurance (QA) and the plant TSs. The CEOG AOT extension efforts for the Safety Injection Tanks (SITs), Low Pressure Safety Injection (LPSI) System, and Emergency Diesel Generators (EDG) (See References B3, B4, and B5) became the pilot documents supporting the development of the Regulatory Guide governing risk-informed changes to the Plant TSs (Reference B6). As experience with risk-informed regulation grew, additional Risk-Informed (RI) AOT extensions have been granted.

In 1998, the NRC proposed that the industry consider a bold initiative to systematically and substantively risk inform the plant TSs. Following a number of NRC sponsored meetings, the industry proposed six risk-informed initiatives for changing the plant TSs. Currently, the industry is sponsoring eight initiatives associated with a Risk Informed Technical Specification (RITS). The discussion provided herein focuses on enabling conditions for the broad based initiative to replace the existing fixed AOTs/CTs with a flexible AOT/CT structure controlled within the plant's 10 CFR 50.65(a)(4) (Reference B7) Maintenance Rule. In the flexible AOT/CT structure, most equipment TS conditions would allow the component outage time to be determined based on the actual plant state, maintenance needs, and relative risks. Specifically, the general features of Initiative 4B of the Risk Management Technical Specification (RMTS) are discussed, and specific risk-informed processes that may be needed for successful implementation of this type of TS are identified. These processes will supplement the existing 10 CFR 50.65(a)(4) program and could be subsumed within that program. Inclusion of these supplementary processes within the plant's maintenance program will enable better integration, and support of the plant TSs. Thus, implementation of these features should provide the necessary processes to enable a smooth transition from current TS with fixed AOTs/CTs to a RMTS with flexible risk-informed AOTs/CTs. The industry effort to transition the TS to flexible completion times is currently defined as Initiative 4B.

It is expected that implementation of RMTS will allow utilities to fully utilize risk-informed tools and processes in the management of plant maintenance. These TS enhancements will reduce plant risk by allowing flexibility in prioritization of maintenance activities, improving resource allocation, and averting unnecessary plant mode changes. The RMTS under development is specifically directed towards equipment outages and will not change the manner in which plant design parameters are controlled.

This Appendix provides the CEOG perspectives on the implementation of the flexible AOT/CT concept and the associated risk management processes.

B2.0 THE MAINTENANCE RULE/TECHNICAL SPECIFICATION NEXUS

Plant Technical Specifications were intended to provide time limits on inoperability of design basis components during various plant modes. These times were designated as AOTs/CTs within TS action statements. In practice, these limits were used to identify what level of maintenance would be done on those components. As refueling outages became shorter, these times were used to help establish the "at power" maintenance durations for design basis and safety related components. While a few selected high-risk maintenance combinations were prohibited by the TS (namely maintenance on redundant trains of the same system), no limitations were provided on non-TS components and most plant configurations were not directly restricted. In some instances, on-line maintenance was primarily based on compliance with the TS AOTs/CTs, and at times resulted in less than desirable plant configurations.

In an effort to improve plant maintenance practices in the nuclear industry, the NRC issued the Maintenance Rule (10 CFR 50.65) as its first risk-informed performance based regulation. The regulation required the licensee to assess and manage risk, including the important contribution of balance of plant non-safety systems. Performance of a risk-informed assessment was not required when the rule was initially issued. In November 2000, the Maintenance Rule was amended with the addition of paragraph (a)(4). Paragraph (a)(4) of 10 CFR 50.65 explicitly required that utilities assess and manage risk in the conduct of maintenance operations. This rule requires that a "risk assessment" be performed prior to voluntary entry into a maintenance configuration, or as soon as practical, upon entry into a non-voluntary maintenance condition. The guidance for satisfying the requirements of this rule provision is defined in Section 11 of NUMARC 93-01 (Reference B8) and has been endorsed by the NRC in RG 1.182 (Reference B9). These guidance documents were built, in part, on the Configuration Risk Management program developed as part of the CEOG pilot for RG 1.177. A companion risk-informed rule (10 CFR 50.59) change associated with evaluating "permanent" plant changes became effective in January 2001 (Reference B10).

As a result of the difference in intent of the TSs and the Maintenance Rule, the control of plant maintenance could be inconsistently treated. For example, the Maintenance Rule provides for a risk assessment prior to voluntary entry into a maintenance configuration, with the emergent work being evaluated as soon as practical. On the other hand, while the TS requires no risk assessment, operation within certain plant configurations is explicitly restricted, require defined

actions and is subject to time restrictions. Furthermore, unlike the TS, the Maintenance Rule is silent on identification of plant conditions requiring plant shutdown.

This risk-informed effort intends to meld the two processes together by replacing the fixed interval AOTs/CTs and prescribed actions in the current TS with a risk-informed alternative. This alternative establishes flexible AOTs controlled by the Maintenance Rule, and shutdown/mode change actions established from a risk assessment process. Thus, TS actions will explicitly consider the contemporaneous plant risks in managing the plant configuration and when conducting restorative actions. The process for assessing plant risks will represent a blending of quantitative information and qualitative considerations.

B3.0 RISK INFORMED TECHNICAL SPECIFICATIONS

B3.1 Historical Evolution

10 CFR 50.36 (Reference B11) requires that the plant's design basis be maintained and that when the plant is outside that design basis, actions be taken to restore that design basis. Plant shutdown is included among the actions to be considered. The regulation has no explicit requirement or process for establishing allowable times for these actions or the associated restorative actions. As the TS evolved, deterministic insights, simplified risk insights, and judgement were used to establish AOTs and actions. However, for the most part, the forced plant shutdown was considered a safe action if design basis compliance could not be restored. The irony of this philosophy is that forced plant shutdown would be required, even when continued plant operation is the lower risk alternative. Later, the TS became increasingly standardized, culminating in the development of the Improved Standard TS (ISTS). The goal of the ISTS was to simplify the TS structure and clarify the TS language. In addition, the ISTS sought to remove conflicts that existed among TS actions and to rationalize some specific TSs by integrating risk insights into the associated actions. While the ISTS resolved many of the initial problems with earlier TS, the actions and allowed outage times (or completion times) remained largely deterministically driven.

Following industry feedback from the 1998 stakeholders meeting, the NRC recommended that the industry consider an initiative to risk inform the plant TS. In response to that initiative, several public meetings were held to identify the aspects of the TS amenable to a risk-informed treatment. Based on these meetings, the NRC and industry have embarked upon an effort to globally risk inform several aspects of the current TS. The product to emerge from this effort is the RMTS. This effort is an outgrowth of the emergence of a "risk conscious" regulatory environment at the NRC and several years of regulatory experience in evaluating and implementing risk-informed changes to the current generation of TSs. As with the existing generation of TSs, the criteria for entry into the associated TS will be defined inoperabilities of a TS System, Structure or Component (SSC). Retention of this structure will ensure that the RMTS is fully compatible with the requirements of 10 CFR 50.36. However, it is envisioned that, once fully implemented, the maintenance related actions for non-TS SSCs will also follow the same risk assessment process.

B3.2 Scope and Structure of the Flexible AOT Concept

The flexible AOT concept is intended to replace the fixed AOT/CT and the prescriptive actions of the current TS with an action statement to conduct a risk-informed assessment. The flexible AOT concept is intended to apply to those TS Action Statements associated with inoperable SSCs within the scope of the TS that currently have ISTS AOTs/CTs of one day or greater. Typically, AOTs/CTs less than one day are associated with loss of system function and extension beyond the existing AOT may incur significant risks. Therefore, shorter term Action Statements, such as those associated with complete system inoperability or loss of an entire safety function will retain an Action Statement with a fixed AOT/CT value based on the system's or function's risk importance. Risk importance may be established using methods consistent with Reference B12. The flexible AOT concept would also not apply to TS associated with plant operational limits.

The structure of the proposed RMTS is illustrated in Table B3-1. Note that the proposed TS makes reference to three time intervals, these are the frontstop AOT/CT, 30 day (or "backstop" completion time), and the acceptable risk time informed interval (implied). The frontstop is the plant's TS AOT/CT as justified via design basis considerations or TS AOT/CT as modified via an approved Reg Guide 1.177 analysis. The 30 day completion time is provided to ensure the plant design basis is retained (that is, no permanent plant changes are made associated with this TS). The 30 day interval is not risk-informed, but rather represents a deterministic limit. The level of acceptable risk beyond the frontstop is established via a risk-informed application of the Maintenance Rule as follows:

1. Prior to exceeding the frontstop AOT, the plant must perform a configuration risk assessment to confirm that the risk of continued operation in the current configuration is acceptable. A quantitative/qualitative risk assessment will provide the basis for continued plant operation. The assessment must consider the impact of common cause failures, external events and flooding.

2. Depending on the outcome of this assessment and assessment of alternative actions, compensatory actions will be defined and the plant will either continue operation beyond the frontstop AOT/CT or shutdown in accordance with TSs. The timing of the plant shutdown will reflect plant cumulative risks, the likelihood of repair, and transition and shutdown considerations.

Quantitative risk assessments will be performed with an appropriately contemporaneous plant model and PSA results should be based on PSAs with minimum Level 1/ Level 2 attributes compatible with the associated risk-informed application. Fire, seismic and or flood risks may be considered qualitatively.

Conceptually, the flexible AOT/CT is simple. For all entries into the TS the licensee will (1) perform a risk assessment in accordance with the Maintenance Rule and in a time frame not to exceed the frontstop AOT, (2) prior to the expiration of the TS frontstop AOT/CT, perform a risk assessment of the inoperability to justify continued power operation beyond the frontstop, (3) based on the results of the risk assessment, take actions to mange risk via expediting repairs,

implementing contingency actions or, initiating a plant shutdown, etc., and (4) once the extended AOT/CT is entered, perform a contemporaneous risk assessment following risk significant plant configuration changes. The risk assessment process will focus on the entire maintenance evolution and will utilize the quantitative action thresholds of Section 11.3.7.2 of Reference B8. In addition, risk assessments will be performed beyond the frontstop AOT/CT to assess the incremental risk of the inoperability associated with maintenance within the extended AOT/CT. These latter results will be tracked, trended and periodically reviewed to ensure the incremental risks of the flexible TS is small (per RG 1.174) and to inform the plant staff of potential deficiencies in the maintenance program. Furthermore, this process will reduce the potential for performing higher risk maintenance beyond the frontstop. For conditions where risk consideration alone would result in a very long AOT/CT, restoration of low risk design basis configurations/equipment will be ensured by the backstop AOT.

B3.3 Basis for "Tiered" AOTs

This section addresses two issues, (1) why a single risk-informed AOT/CT (typical of RG 1.177) is not used for the RMTS and (2) why it is recommended that the backstop completion time is fixed and not risk based. In performing risk-informed assessments to extend AOTs/CTs per the requirements of RG 1.177 it must be assumed that the component in question is entirely inoperable. Furthermore, while the component is inoperable it must be shown that the resulting allowable risk increment is small. In the PSA this inoperability is evaluated as a complete non-functionality of the system. That is, during the AOT/CT the SSC in question will not be capable of performing its mitigation function. Under these circumstances the risk associated with the inoperability and the associated AOT/CT is established. In practice, SSC inoperabilities are not extensive and result in equipment being declared inoperable with various levels of residual capabilities. For a HPSI train, for example, typical failure modes that result in partial system inoperability include, but are not limited to:

- Degradation / unavailability of local Heating, Ventilation and Air Conditioning (HVAC),
- Inoperability of various automatic functions (when manual override is available and timely),
- Limited degradation component capability (e.g. delivery),
- Unavailability of one or more multiple flowpaths,
- Unavailability or impairment of adverse event protection (flood, fire, High Energy Line Break (HELB)), or
- Inoperability of one mode of operation where a system has multiple modes.

In the above circumstances, the accumulated risks may be considerably lower than determined in setting the risk-informed AOT/CT where full inoperability is assumed. Furthermore, many failure modes may be partly addressed via implementation of appropriate contingency actions. Operational risks can be established using risk-informed assessment techniques for the current plant configuration. Since only partial degradation occurs in many instances, time for repair / replacement can be safely extended.

While it is expected that most planned and exigent maintenance activities will be successfully completed within the frontstop AOT/CT, availability of a flexible AOT/CT will allow plants to

more confidently schedule low risk maintenance closer to the frontstop AOT/CT limits. This will allow more efficient scheduling of maintenance tasks. Planned maintenance beyond the frontstop AOT/CT should be infrequent, although repair/replacement operations beyond that time may be advantageous from both a risk perspective and plant availability perspective. Such issues may arise during low risk maintenance evolutions, when post-maintenance tests indicate an operational deficiency or a replacement part is unavailable. As discussed above, the proposed risk-informed AOT/CT includes a process for justifying this extended operation and establishing its risks. However, in rare circumstances it may not be possible to accomplish a low risk repair in an acceptable time. A 30 day backstop limit is included to ensure action to repair/replace the SSC is forthcoming and to prevent an after-the-fact design change by leaving low risk TS components out of service indefinitely.

Table B3-1
Generic Risk Informed AOT's with a Backstop: Example Format

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
B. One HPSI train inoperable.	B.1	Restore inoperable HPSI train to OPERABLE status.	72 hours
		OR	
	B.2.1	Determine that the risk configuration is acceptable for completion time extension beyond 72 hours.	72 hours
		AND	
	B.2.2	Determine that the risk configuration remains acceptable beyond 72 hours.	Whenever configuration changes that affect plant risk occur.
		AND	
	B.2.3	Restore inoperable HPSI train to OPERABLE status.	Acceptable completion time extension or 30 days, whichever is less.

B3.4 Tracking of Risks

The cumulative incremental risk associated with this TS change will be controlled by setting low individual risk targets beyond the frontstop and tracking of the incremental risks to ensure the impact of the TS modification remains small. Maintenance Rule self assessment processes will be used to control specific maintenance evolutions and maintain acceptable baseline risk. Additionally appropriate application may be reviewed within the Safety Function Determination Process via Risk Informed Plant Indicators. To ensure control of cumulative risks individual

maintenance activities beyond the frontstop should be targeted for loss incremental single use increases. That is, the core damage probability within the extended AOT/CT should be targeted to approximately 1.0E-06 and the incremental large early release probability to approximately 1.0E-07. At these levels, operation within the extended AOT will not have a significant adverse risk impact. As maintenance activities beyond the frontstop will be infrequent, controlling individual maintenance risks at this level will ensure RG 1.174 annual guidelines will not be challenged. To be consistent with RG 1.174 the impact on the plant yearly risk profile, level of incremental risk should be limited to changes in CDF and LERF of less than 1.0E-5 per year and less than 1.0E-06, respectively. These incremental risk goals are considered guidelines. In estimating the adherence to these guidelines, the assessments may consider, as appropriate, proceduralized compensatory measures, operator actions and alternative offsetting risks in utilizing the extended AOT. Administrative assessments of the risk impact of the extended AOT/CT will be performed and significant findings will be subsumed into the plant's corrective action program. Specific quantitative tracking of the extended AOT/CT is not considered necessary when maintenance ICDPs remain in the region of normal plant controls (ICDP < 1.0E-06) for the entire outage configuration. Under this circumstance, tracking may be limited to the duration of the extended AOT/CT entry.

B3.5 Elements of the Risk Assessment Process

The underpinning of the flexible AOT/CT is the plant's risk assessment and management program. The risk assessment process performed to support the flexible AOT is envisioned as a robust application of 10 CFR 50.65(a)(4), supplemented by (1) a risk-informed screening process to identify high risk plant configurations, (2) expedited assessment of common cause potential for emergent conditions, and (3) processes for controlling and assessing risk beyond the frontstop AOT. When available, risk-informed shutdown mode change assessments may be utilized to define risks associated with alternative actions. The process will be evoked for all entries into the RMTSs.

B3.6 Example

One example of how the flexible AOT may be used is provided in the instance of unavailability of a single injection valve in the high pressure safety injection (HPSI) system. In the Combustion Engineering (CE) fleet each HPSI train injects Safety Injection (SI) flow into a header with four injection lines directing the SI flow to each of the four Reactor Coolant System (RCS) cold legs. "MOVAT" testing on these valves nominally requires 50 hours during which time the associated HPSI train is tagged inoperable. Additional maintenance and retesting would be required should test results prove inadequate. Such an activity can result in exceeding the current frontstop AOT. Depending on plant design, complete inoperability of the HPSI train will result in a 3-day AOT/CT risk of between 1.0E-07 to less than 1.0E-06. However, focused analyses of the removal of the single injection valve from service for a period of seven days will result in an incremental core damage probability of less than 1.0E-08. The risk increment would be small even if this maintenance were to extend to 30 days. As a result of the low importance of the HPSI on mitigating fire and seismic induced events, the impact of (non-internal) event risks would be negligible. Additional examples may be found in Section 6 of the main report.

In performing this maintenance, the flexible AOT/CT process would utilize existing maintenance rule processes. Once an extended time entry is required, a contemporaneous configuration specific risk assessment will be performed and a decision to complete the repairs at power will be made. The decision will consider the current plant risk, likelihood of a successful repair (i.e. availability of injection lines, etc.) and alternative actions. Compensatory actions will be considered prior to entry into the extended AOT/CT and implemented, as necessary.

Once the repair enters the extended AOT/CT, a risk assessment defining the incremental CDP and LERP associated with the extended repair will be generated and recorded for future review. Re-assessments will be performed following risk significant plant configuration changes. Tracking assessments will be concluded once the component is returned to service. This tracking process may or may not be directly associated with the plant contemporaneous plant maintenance risk. The overall maintenance risk will continue to be governed by standard Maintenance Rule practices.

While it is not the intent of the flexible AOT to delay component repair, actual risk information and flexibility in assessing the impact of and removing equipment from service will allow risk-informed prioritization for repairs and minimize the need for cycling the plant and regulatory staffs to formally secure a Notice of Enforcement Discretion (NOED) for low risk conditions. A thirty day limit is provided such that no matter how low the component risk is, the plant design basis will be preserved.

B4.0 OVERVIEW OF THE (a)(4) PROCESS

10 CFR 50.65 paragraph (a)(4) states that before performing maintenance activities (including but not limited to surveillances, post-maintenance testing, and corrective and preventive maintenance), the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. Risk assessments are not limited to equipment inoperability and can include equipment troubleshooting, hazard barrier removal, erection of scaffolding, lifting electrical leads and installing electrical jumpers. The scope of the assessment may be limited to systems, structures and components that a risk-informed evaluation process has shown to be significant to public health and safety. Furthermore, the (a)(4) plant maintenance evaluation is required for all plant operating modes and considers the impact of external events. Additional details of this process are contained in NUMARC-93-01 (Reference B8).

The (a)(4) process should:

1. Be documented in plant procedures delineating appropriate responsibilities for (a)(4) related actions.
2. Result in a consistent decision making process.
3. Include a risk assessment as an integral part of the maintenance work control process.
4. Include procedures for performing a risk assessment when the maintenance items are outside the scope of the quantitative risk assessment tool.

5. Define a process so that when the plant configuration is outside the scope of the (a)(4) tool, or the tool is otherwise unavailable, qualitative methods may be used to assess risk and define appropriate actions to manage the risk increase.
6. Include guidance for using risk insights to manage overall plant risk.

In performing the (a)(4) assessment, the decision making process may optimally include consideration of transition risks associated with mode changes.

Implementation of the (a)(4) risk assessment process requires integration into the plant-wide work control process to identify the current plant configuration, perform a risk assessment applicable to that configuration and take appropriate actions to manage the risk impacts.

The remainder of this document assumes that the plant is fully compliant with 10 CFR 50.65(a)(4). It is further assumed that the plant risk assessments integrate PSA results and PSA derived risk insights into the process. The supplementary processes discussed in this report are intended to enhance the existing (a)(4) process in order to allow it to accommodate a greater plant control function. The primary intent of these processes is to ensure that selected desirable attributes of the current TSs are retained in the RMTS structure in a risk-informed format. These attributes include:

- Preservation of the ISTS Structure.
- Reliance on defined time interval limits (i.e., frontstop AOT).
- Reference to defined actions in the TS LCO.

B5.0 INITIATIVE 4B ENHANCEMENTS

This section describes a proposed integration of the present 10 CFR 50.65(a)(4) evaluation process with selected supplementary processes to create a process to support the implementation of Flexible AOTs/CTs within the plant TSs. The specific features/processes to be added into the (a)(4) risk management process include:

1. Identification of, and timely response to, emergent High Risk conditions.
2. Implementation of a formal Risk Informed Decision Process for plant shutdown/mode change.

The first feature is added to ensure that a delay in the risk assessment (up to the time of the frontstop) will not result in the emergence of a high risk plant configuration. The second process is defined to support the assessment that the "configuration is acceptable for continued operation."

The addition of these processes to the existing 10 CFR 50.65(a)(4) (where they do not already exist) will facilitate the transition to flexible AOTs/CTs.

B5.1 Comments on the Integration of Initiative 4B with 10 CFR 50.65(a)(4)

The integrated process is intended to provide a comprehensive risk-informed mechanism for expeditious identification of risk significant plant conditions and the implementation of appropriate risk-informed maintenance actions, and may include the action to shutdown the plant. In practice this program is transparent for all 10 CFR 50.65(a)(4) maintenance planning conditions. That is, the program retains the current 10 CFR 50.65(a)(4) practice, which prohibits the plant from voluntarily entering high risk conditions without proper evaluation of the concurrent risks and implementation of appropriate management actions.

The initiative 4B process enhancements will be initiated upon entry into an emergent unevaluated condition. The first step in the process is the identification of the plant state. To do this the plant needs an adequate Maintenance Rule process, knowledge of ongoing maintenance activities including significant Out of Service equipment, and an understanding of the potential for significant common cause failures. Once the plant condition is known, an initial screening risk assessment of the current plant configuration against previously identified high risk configuration is performed. The purpose of this screening is to rapidly identify the presence of a high risk[3] plant evolution. Risk management actions will be provided for high risk conditions including plant shutdown.

Once the potential for a high risk condition is eliminated, a risk assessment will be performed and normal maintenance rule processes will be followed. Based on the results of this assessment, risk management actions will be identified, prioritized and implemented. Risk management actions can include expedited repair of selected equipment, and assessment of the status of redundant standby equipment, etc. Potentially high risk conditions are further considered for a shutdown assessment. Lower risk evolutions are treated via the current 10 CFR 50.65(a)(4) program with a time frame commensurate with their risk significance. In order to maintain industry and NRC plant performance goals with respect to unavailability and risk, it is expected that most maintenance will be conducted within the default (frontstop) AOT/CT. In instances when the frontstop AOT/CT is exceeded, the integrated process will ensure that the continued component outage does not significantly impact risk and that appropriate actions are taken to expeditiously return affected equipment to service.

The yearly risk of operation beyond the frontstop will be tracked and administratively evaluated on a periodic basis, consistent with the Maintenance Rule self assessment. Incremental CDFs associated with the flexible AOTs/CTs should be consistent with RG 1.174 annual guidance.

B6.0 PSA CONSIDERATION/ATTRIBUTES

Use of the flexibility afforded in the RITS structure is tied to the capability of the plant's risk assessment process. Prior to implementing RITSs, the plant's "at power" PSA will have undergone a peer review to ensure that the current PSA model reflects the as-built plant with system dependencies and the plant operating practices considered. The PSA internal events

[3] High risk conditions are those which typically result in instantaneous on the order of 1.0E-03 per year (See Reference B8) or situations which result in the loss of a safety function.

review should be consistent with NEI-99-002 (Reference B13) or its equivalent and also the ASME PSA Standard (Reference B14). The risk assessment process should also appropriately disposition peer review comments with significant issues being corrected or compensated. In order to effectively utilize the flexible portion of the AOT/CT, maintenance-related risk insights from fire and external event assessments should be integrated into the risk assessment process. This may be done quantitatively via integrating dominant fire, and external event risk sequences into assessment tools, or qualitatively, by including associated risk insights into pre-maintenance checklists and use of expert judgement.

The plant's 10 CFR 50.65(a)(4) (including associated Initiative 4B enhancements) program should include or reference processes for adequately identifying and evaluating the current plant state. The plant should also have a risk-informed program for identifying, tracking and assessing risk significant plant design changes. The configuration control process should include interfaces with the plant's corrective action program to ensure that significant deficiencies in the program are identified and resolved.

Prior to implementation of the process, a listing of high risk states (not prohibited by the current TSs) should be identified and/or a demonstration of the capability of the tool to evaluate the plant configuration and schedule should be conducted. Such assessments may include limited perturbation assessments for a typical maintenance cycle.

B7.0 COMMENTS REGARDING IMPLEMENTATION OF RISK ASSESSMENT TOOL

Risk Managed Technical Specifications should be able to be implemented by PWRs and BWRs with a robust risk-informed 10 CFR 50.65(a)(4) program. It is envisioned that RMTS implementation will not require instantaneous on-line assessments or precise numerical risk estimates. However, processes to accommodate longer assessment times (including pre-assessment and identification of high-risk conditions that would require short-term assessments) and compensatory actions to address model limitations should be in place. The scope of actions available to the plant and the breadth of decisions may also be limited by the availability and scope of assessment tools. This feature would allow greater flexibility in implementation to accrue to those plants with more robust capabilities.

Many of the plants utilizing the flexible AOT/CT will have robust Level 1 PSAs and risk insights associated with fire, seismic and external flooding assessments. External event insights may be treated qualitatively via use of risk insight related checklists. The PSA should be peer reviewed in accordance with NEI-00-002 with identified weaknesses resolved or otherwise taken into account.

It is recommended that prior to implementation of the RMTS ("flexible AOT"), a demonstration of the risk-informed evaluation and control processes be performed. This demonstration may include limited post assessment of previous cycles' maintenance, or assessment of past NOEDs and a demonstration of how such situations would be handled when the RMTS process is instituted. In addition, a set of pre-defined failures of TS components can be postulated in the

process of a normal maintenance schedule and the impact of delayed repair on plant risk and actions should be evaluated. Results of these studies may be used to inform the utility and NRC staff of the plant's program for implementing the flexible AOT/CT.

B8.0 REFERENCES

B1. CEN-327-A, "RPS/ESFAS Extended Test Interval Evaluation," May 1986.

B2. WCAP-10271-P-A, "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System," May 1986.

B3. CE-NPSD-994, "Safety Injection Tanks AOT," CEOG Task 836, May 1995.

B4. CE-NPSD-995, "Low Pressure Safety Injection System AOT," CEOG Task 836, April 1995.

B5. CE NPSD-996, "Emergency Diesel Generator AOT," CEOG Task 836, April 1995.

B6. RG 1.177, "An Approach for Plant Specific, Risk-Informed Decisionmaking: Technical Specification," NRC August 1998.

B7. 10 CFR 50.65, "Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plant," NRC, (56 FR 31324 dated July 10, 1991).

B8. NUMARC 93-01, Revision 3, "NEI Industry Guidelines for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," NEI, July 2000.

B9. RG 1.182, "Assessing & Managing Risk before Maintenance Activities at Nuclear Power Plants," NRC, May 2000.

B10. NEI 96-07, Revision 1, "Guidelines for 10 CFR 50.59 Implementation," November 2000.

B11. 10 CFR 50.36, "Technical Specifications," Code of Federal Regulations NRC.

B12. CE-NPSD-1208, "Justification of Risk Informed Modifications to Selected Technical Specifications for Conditions Leading to Exigent Plant Shutdown," December 2000 Westinghouse, Inc.

B13. NEI-00-002, "Probabilistic Risk Assessment Peer Review Process Guideline," NEI, April 1, 2000.

B14. CEOG Certification, "Standard for Probabilistic Risk Assessment for Nuclear Power Plants," Revision 14A, ASME, May 11, 2001.

WCAP-15773-P, Rev 00
Westinghouse Proprietary Class 2

Westinghouse Electric Company LLC
2000 Day Hill Road
Windsor, CT 06095-0500