Westinghouse Non-Proprietary Class 3

WCAP-15377-NP-A
Revision 1

March 2003

Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times

Westinghouse

NRC Safety Evaluation

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

December 20, 2002

Mr. Robert H. Bryan, Chairman
Westinghouse Owners Group
Tennessee Valley Authority
Mail Code LP4J-C
6A Lookout Place
1101 Market Street
Chattanooga, TN 37402-2801

SUBJECT: ACCEPTANCE FOR REFERENCING OF TOPICAL REPORT WCAP-15376-P, REV. 0, "RISK-INFORMED ASSESSMENT OF THE RTS AND ESFAS SURVEILLANCE TEST INTERVALS AND REACTOR TRIP BREAKER TEST AND COMPLETION TIMES" (TAC. NO. MB0983)

Dear Mr. Bryan:

By letter dated November 8, 2000, as supplemented by letters dated June 8, June 25, and September 28, 2001, and January 8, 2002, the Westinghouse Owners Group (WOG) submitted the subject topical report (TR) prepared by Westinghouse Electric Company, LLC, that revises the technical specifications for the reactor trip system and engineered safety features actuation system instrumentation. The proposed changes include increasing the completion time and bypass time for the reactor trip breakers, as well as the surveillance test intervals for the reactor trip breakers, master relays, logic cabinets, and analog channels. The proposed changes adopt the staff's approved Technical Specification Task Force (TSTF) Traveler TSTF-411, Rev. 1, "Surveillance Test Interval Extension for Components of the Reactor Protection System," submitted by letter dated August 9, 2001.

The NRC staff has completed its review of the subject TR. The TR is acceptable for referencing in licensing applications to the extent specified and under the limitations delineated in the report and in the associated NRC safety evaluation (SE), which is enclosed. The enclosed SE defines the basis for acceptance of the TR.

The staff has concluded that the proposed generic TS changes are consistent with the approved allowances for testing with an instrument channel in bypass and for repair completion times accepted by the staff based on WCAP-15376-P. In addition, proposed TS Bases provide an adequate basis or reason for the standard technical specification (STS) changes. Therefore, Westinghouse should include TSTF-411, Rev. 1, with publication of the approved version of WCAP-15376-P. Licensees may then propose to adopt the approved TS during a conversion to the STS or as a separate license amendment application for WCAP-15376-P.

Pursuant to 10 CFR 2.790, we have determined that the enclosed SE does not contain proprietary information. However, we will delay placing the SE in the public document room for ten working days from the date of this letter to provide you with the opportunity to comment on the proprietary aspects only. If you believe that any information in the enclosure is proprietary, please identify such information line by line and define the basis pursuant to the criteria of 10 CFR 2.790.

We do not intend to repeat our review of the matters described in the subject report, and found acceptable, when the report appears as a reference in license applications, except to ensure that the material presented applies to the specific plant involved. Our acceptance applies only to matters approved in the report.

In accordance with the procedures established in NUREG-0390, the NRC requests that the WOG publish an accepted version within three months of receipt of this letter. The accepted version shall incorporate (1) this letter and the enclosed SE between the title page and the abstract, (2) all requests for additional information from the staff and all associated responses, and (3) a "-A" (designating "accepted") following the report identification symbol.

Should our criteria or regulations change so that our conclusions as to the acceptability of the report are invalidated, the WOG and/or the licensees referencing the TR will be expected to revise and resubmit their respective documentation, or submit justification for the continued applicability of the TR without revision of their respective documentation.

Sincerely,

William H. Ruland

William H. Ruland, Director
Project Directorate IV
Division of Licensing Project Management
Office of Nuclear Reactor Regulation

Project No. 694

Enclosure: Safety Evaluation

cc w/encl:
Mr. Gordon Bischoff, Project Manager
Westinghouse Owners Group
Westinghouse Electric Company
Mail Stop ECE 5-16
P.O. Box 355
Pittsburgh, PA 15230-0355

Mr. Hank A. Sepp, Jr.
Manager, Regulatory & Licensing
Westinghouse Electric Company
Nuclear Services
P.O. Box 355
Pittsburgh, PA 15230-0355

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

WCAP-15376-P, REV 0, "RISK-INFORMED ASSESSMENT OF THE RTS AND ESFAS SURVEILLANCE TEST INTERVALS AND REACTOR TRIP BREAKER TEST AND COMPLETION TIMES"

WESTINGHOUSE OWNERS GROUP

PROJECT NO. 694

1.0 INTRODUCTION

By letter dated November 8, 2000, and its supplemental letters dated June 8, June 25, September 28, 2001, and January 8, 2002, the Westinghouse Owners Group (WOG) submitted WCAP-15376-P, Rev. 0, "Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times." WCAP-15376-P, Rev. 0, provides justification for increasing the allowed outage time (AOT)/completion time (CT) and bypass times for the reactor trip breaker (RTB), as well as the surveillance test interval (STI) for the RTB, master relays, and logic cabinets.

The proposed changes adopt the Nuclear Energy Institute (NEI) Technical Specifications Task Force (TSTF) Traveler TSTF-411, Rev. 1, "Surveillance Test Interval Extension for Components of the Reactor Protection System," submitted by letter dated August 9, 2001.

The CT is defined as part of the limiting condition for operation (LCO) in the improved standard technical specifications (STSs). The AOT is a general reference to time to accomplish a technical specification (TS) required Action. To have more specific meaning, AOT can refer to additional time for repair, bypass, shutdown, etc. A CT has a broader meaning than an AOT, by also defining the time for other required actions such as equipment status or plant mode changes. The CT is intended to allow sufficient time to repair failed equipment while minimizing the risk associated with the loss of the component function.

The purpose of the program is to provide the technical justification for extending the STI for components for the reactor protection system. The components specifically included are analog channels, logic cabinets, master relays, and reactor trip breakers. This program also provides the technical justification for extending the RTB completion time (allowed outage time) for one RTB inoperable to 24 hours from 1 hour and the bypass time for an RTB to 4 hours from 2 hours. This safety evaluation considers both the solid state protection system (SSPS) and relay protection system. An extension of the STI reduces the required testing on the reactor protection system components without significantly impacting its reliability, and reduces the potential for reactor trips and actuations of engineered safety features associated with the testing of these components. An extension of the CT increases the unavailabilty of a component due to the increased time the component is down for maintenance. The CT risk is reflected in the core damage frequency (CDF) and the large early release frequency (LERF) by adjusting the component unavailability due to maintenance. The CT extensions for the RTB will provide the licensees additional time to complete test and maintenance activities while at power, potentially reducing the number of forced outages related to compliance with reactor trip breaker CTs, and provide consistency with the CTs for the logic cabinets. For CTs, the designated CTs may not provide adequate time for repair, but longer CTs may incur a relatively larger risk. Note that the STS replaced the term AOT with CT, which has a broader meaning than AOT by also defining the time for other required actions such as equipment status or plant mode changes.

By contrast, STIs are intervals for surveillance tests scheduled periodically as required by the TS. Such tests are performed to ensure that safety-related equipment continues to be operable and failures are detectable, thereby limiting the fault exposure time. The primary risk contribution attributed to increasing an STI comes from the increased probability of a component failure between scheduled STIs and, therefore, the probability that the component will be inoperable during the surveillance interval. The extension of an STI affects the yearly risk, which is represented by the CDF and LERF. An STI extension can affect the yearly risk in several ways:

- Reduce the risk by decreasing the number of test-caused reactor trips by limiting the opportunity for test-caused errors. This occurs simply because increasing the STI decreases the amount of testing for a given time.

- Reduce the risk by decreasing the unavailability of the reactor protection system (RPS) component by reducing the test frequency.

- Increase the risk by increasing the fault exposure time as described above. This is attributable to the fact that the increased STI increases the interval during which the equipment is subject to failure during standby. As the fault exposure time increases, there is a greater probability that failures during standby will not be detected for RPS components involved with the STI extension.

For an STI, the idea is to strike a balance between more frequent testing (which can adversely impact safety either through errors during testing, spurious actuations, misconfiguration, or equipment wearout) and extended intervals (which can increase fault exposure times). The designated CTs may not provide adequate time for repair, but longer CTs may incur a relatively larger risk. A risk-informed approach to CTs and STIs in conjunction with engineering evaluations, can provide insights that allow CTs and STIs to be optimized without significantly increasing plant risk.

The NRC's policy statement on the use of probabilistic risk assessment (PRA) methods in nuclear regulatory activities encourages the use of PRA to improve safety-related decision-making and regulatory efficiency. Under this policy, the NRC staff may use traditional engineering analysis, as well as risk-informed approaches, to evaluate licensee-initiated licensing changes that go beyond current staff positions. In WCAP-15376-P, Rev. 0, the WOG stated that the proposed changes to the STIs will reduce the required testing on RPS components without significantly impacting the reliability of the reactor trip system (RTS), while reducing the potential for reactor trips and actuation of engineered safety features associated with the testing of these components. The WOG also stated that extending the CTs for the RTBs will provide additional time to complete test and maintenance activities while at power, and provide consistency with the CT for the logic cabinets.

The proposed increases in STIs, CTs, and bypass times for both the SSPS and relay protection system RTS and associated engineered safety features actuation system (ESFAS) designs are as follows:

(1) SOLID STATE PROTECTION SYSTEM

- Surveillance Test Intervals

Logic cabinet:	From 2 months to 6 months
Master Relay:	From 2 months to 6 months
Analog Channels:	From 3 months to 6 months
Reactor Trip Breaker:	From 2 months to 4 months

- Completion Time

Reactor Trip Breakers:	From 1 hour to 24 hours

- Bypass Times

Reactor Trip Breakers:	From 2 hours to 4 hours

(2) RELAY PROTECTION SYSTEM

- Surveillance Test Intervals

Logic Cabinet:	From 1 month to 6 months
Master Relay:	No change
Analog Channels:	From 3 months to 6 months
Reactor Trip Breakers:	From 2 months to 4 months

- Completion Time

Reactor Trip Breakers:	From 1 hour to 24 hours

- Bypass Time

Reactor Trip Breakers:	From 2 hours to 4 hours

Whereas the CT is the additional time that is available to correct a fault that is discovered during testing and the bypass time is defined as the amount of time a component can be bypassed for surveillance testing.

Depending on the plant protection system design, some of the actuation logic and master relays associated with the containment purge and exhaust isolation instrumentation (STS 3.3.6) and control room emergency filtration system (CREFS) actuation instrumentation (STS 3.3.7) TSs may be processed through the relay or solid state protection system. Since the STIs for the actuation logic and master relays of the ESFAS Instrumentation were justified to be relaxed in this report, these STI relaxations are also applicable to the actuation logic and master relays for all signals processed through the relay or SSPS.

The STI for the source range neutron flux channel operational test (COT) in the RTS instrumentation (STS 3.3.1) TS was justified to be relaxed in this report. Since this source range neutron flux channel is also used for the boron dilution protection system (BDPS) (STS 3.3.9), the STI relaxation is also applicable to that STI.

The approach used in this program is consistent with the NRC's approach for using PRA in risk-informed decisions on plant-specific changes to the current licensing basis as presented in Regulatory Guides (RGs) 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," and 1.177, "An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specification." The approach addresses the impact on defense-in-depth and the impact on safety margins, as well as an evaluation of the impact on risk. The risk evaluation considers the three-tiered approach as presented in RG 1.177 for the extension to the RTB CT. Tier 1, PRA Capability and Insights, assesses the impact of the proposed CT (AOT) change on CDF, incremental conditional core damage probability (ICCDP), LERF, and incremental conditional large early release probability (ICLERP). Tier 2, Avoidance of Risk-Significant Plant Configurations, considers potential risk-significant plant operating configurations. Tier 3, Risk-Informed Plant Configuration Control and Management, will be addressed on a plant-specific basis when the TS CT change is implemented by each licensee.

2.0 REGULATORY EVALUATION

The NRC staff formed a task group in August 1983 to investigate problems and recommend improvements concerning surveillance testing required by TS. The results of the Task Group study were published in November 1983 in NUREG-1024, "Technical Specifications-Enhancing the Safety Impact." NUREG-1024 recommended that the staff (1) review the bases for TS test frequencies, (2) ensure that the TS required tests promote safety and do not degrade equipment, and (3) review surveillance tests to ensure that they do not unnecessarily burden personnel.

The technical specification improvement program (TSIP) was established in December 1984 to provide the framework for addressing the recommendations of NUREG-1024, and for rewriting and improving the STS. The results of the TSIP were documented in NUREG-1366, "Improvements to Technical Specifications Surveillance Requirements." The TSIP study concluded that, while some testing at power is essential, safety can be improved, equipment degradation decreased, and unnecessary personnel burden prevented by reducing the amount of testing performed at power.

In 1983, the WOG submitted WCAP-10271-P, "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System," which provided a methodology to be used to justify revisions to a plant's TS. The WOG Technical Specification Optimization Program (TOP) evaluated changes to surveillance test intervals and allowed outage times for the analog channels, logic cabinets, master and slave relays, and reactor trip breakers. The methodology evaluated increasing surveillance intervals, increases in test and maintenance out-of-service times and bypassing portions of the RPS during test and maintenance. The WOG stated in WCAP-10271-P that plant staff devote significant time and effort to perform, review, document, and track surveillance activities that, in many instances, may not be required on the basis of the high reliability of the equipment. The justification for the changes was the small impact that the changes would have on plant risk.

In WCAP-10271-P, the WOG performed fault tree analyses to calculate the reactor trip unavailability considering surveillance intervals and test and maintenance times. The sensitivity to variations in surveillance intervals and test and maintenance times was also evaluated with respect to maintaining or revising current surveillance intervals. The WOG concluded that the results of the analyses for the RPS were adequate to justify a revision of the STS. The staff accepted WCAP-10271-P by safety evaluation report (SER), with provisions, dated February 21, 1985, in which the staff approved the following changes for plant-specific TS:

1. Increase the surveillance interval for RTS analog channel operational tests from once per month to once per quarter.

2. Increase the time in which an inoperable RTS analog channel may be maintained in an untripped condition from 1 hour to 6 hours.

3. Increase the time an inoperable RTS analog channel may be bypassed to allow testing of another channel in the same function from 2 hours to 4 hours. Also, the channel test may be done in the bypass mode leaving the inoperable channel in tripped condition.

4. Allow testing of the RTS analog channels in a bypass condition instead of a tripped condition.

Subsequent to the approval of WCAP-10271-P, the WOG submitted WCAP-14333-P, "Probabilistic Risk Analysis of the RPS and ESFAS Test Times and Completion Times," dated May 1995. The purpose of this WCAP was to evaluate the following changes to the TS:

1. Increase the bypass times and the CTs for both the solid state and relay protection system RPS and ESFAS designs: (i) for the analog channels the CT increased from 6 hours to 72 hours, and the bypass time from 4 hours to 12 hours, and (ii) for the logic cabinets, master and slave relay CTs were increased from 6 hours to 24 hours.

2. Revise the action statement for an inoperable slave relay to increase the CT for maintenance to 24 hours, with an additional 6 hours for the mode change.

3. For cases where the logic cabinets and the trip breakers both cause their train to be inoperable when in test or maintenance, allow the reactor trip breakers to be bypassed for the period of time equivalent to the bypass time for the logic cabinets, provided that both are tested at the same time.

The staff approved WCAP-14333-P by SER dated July 15, 1998, subject to the condition that licensees confirm the applicability of the WCAP to their plant, and that licensees address RG 1.177, Tier 2 and Tier 3 analysis, including the incorporation of applicable Configuration Risk Management Program (CRMP) insights.

To facilitate the implementation of risk-informed methodology, general guidance for evaluating the technical basis for proposed changes is provided in Chapter 19.0 of the Standard Review Plan (SRP). More specific guidance related to risk-informed TS changes is provided in Section 16.1 of the SRP. Chapter 19.0 of the SRP states that a risk-informed application should be evaluated to ensure that the proposed changes meet the following key principles:

1. The proposed change meets the current regulations, unless it explicitly relates to a requested exemption or rule change.

2. The proposed change is consistent with the defense-in-depth philosophy.

3. The proposed change maintains sufficient safety margins.

4. When proposed changes increase core damage frequency or risk, the increase should be small and consistent with the intent of the Commission's Safety Goal Policy Statement.

5. The impact of the proposed change should be monitored using performance measurement strategies.

With respect to the above principles for risk-informed licensing basis changes, RG 1.174 and RG 1.177 identify a four-element approach for use in evaluating a plant's design, operations, and other activities associated with evaluating risk-informed regulatory changes:

Element 1: Define the Proposed Change

When defining the proposed change, a requested TS change may be acceptable if it (1) improves operational safety, (2) can be supported on the basis of risk implications, and/or (3) reduces unnecessary regulatory burden.

Element 2: Perform an Engineering Analysis

RG 1.174 states that the technical basis for the proposed change should be rooted in traditional engineering and system analysis. The proposed TS change should not be based solely on PRA results.

Element 3: Define Implementation and Monitoring Program

The licensee should develop and define a CRMP. This program is to be used to ensure that risk-significant plant configurations will not be entered, and appropriate actions are available if unforeseen events put the plant in a risk-significant configuration. The CRMP should ensure that an extension of a TS CT or STI does not degrade operational safety over time. Additionally, the licensee's Maintenance Rule program should ensure that when equipment does not meet its performance criteria, an evaluation of the equipment associated with the CT or STI will be performed.

Element 4: Submit Proposed Change

The proposed TS change should be documented and included in the licensee's amendment request, and should include risk-informed TS change documentation showing that the objectives of the NRC's PRA policy statement are being met and are consistent with the key principles and elements of RGs 1.174 and 1.177.

As part of Element 2, RG 1.177 identifies a three-tiered approach for a licensee to evaluate the risk associated with a proposed TS change:

- Tier 1 is an evaluation of the plant-specific risk associated with the proposed TS change, as shown by the change in CDF and ICCDP. Where applicable, containment performance should be evaluated on the basis of an analysis of LERF and ICLERP.

- Tier 2 identifies and evaluates, with respect to defense-in-depth, any potential risk-significant plant equipment outage configurations associated with the proposed change. The licensee should provide reasonable assurance the risk-significant plant equipment outage configurations will not occur when equipment associated with the proposed TS change is out-of-service.

- Tier 3 provides for the establishment of an overall CRMP and confirmation that its insights are incorporated into the decisionmaking process before taking equipment out-of-service prior to or during the CT. Compared to Tier 2, Tier 3 provides additional coverage on the basis of any additional risk-significant configurations that may be encountered during maintenance scheduling over extended periods of plant operation. Tier 3 guidance can be satisfied by the Maintenance Rule, 10 CFR 50.65(a)(4), which requires a licensee to assess and manage the increase in risk that may result from activities such as surveillance, testing, and corrective and preventive maintenance.

On February 6, 1987, the Commission issued guidelines for improving the content and quality of nuclear power plant TS, "Interim Policy Statement on Technical Specification Improvements for Nuclear Power Reactors" (52 FR 3788). During the period from 1989 to 1992, utility owners groups and the staff developed improved STS that would establish models of the Commission's policy for each primary reactor type.

In September 1992, the Commission issued Revision 0 of the improved STS as NUREGs 1430-1434, which were developed using the guidance and criteria contained in the Commission's Interim Policy Statement. The ISTS reflect the results of a detailed review of the application of the interim policy statement criteria to generic system functions, which were published in a "Split Report" issued to the nuclear steam supply system (NSSS) vendor owners groups in May 1988.

In June 2001, Revision 2 of NUREG-1431, "Standard Technical Specifications, Westinghouse Plants," was published. The changes to Revision 1 that are reflected in Revision 2 resulted from the experience gained from license amendment applications to convert to these improved STS or to adopt partial improvements to existing technical specifications. NUREG-1431, Revision 2 is the result of extensive public technical meetings and discussions between the

NRC staff and various nuclear power plant licensees, NSSS vendors owners groups and the NEI TSTF.

The review of proposed generic changes to Westinghouse STS (NUREG-1431) is a multi-staged process designed to ensure that each STS remains internally consistent, maintains coherence among the various vendor's STS, and incorporates the knowledge and operating experience of the industry and the NRC. Changes to the STS NUREGs, which are potentially applicable to multiple plants, are proposed to the NRC by the NEI sponsored TSTF through publicly available submittals. The TSTF includes representatives from the four U.S. commercial nuclear power plant owner groups and NEI. The NRC staff reviews the changes to the STS proposed by the TSTF (referred to as TSTF changes) and will accept, modify, or reject them. Once TSTF changes are accepted, they are considered to be part of the STS. Individual licensees may propose to adopt the TSTF changes during a conversion to the STS or as a separate license amendment application.

The TSTF process facilitates licensees adopting NRC-accepted changes to the STS for their specific plant TS. This process is intended to streamline the license amendment review process involving NRC-accepted STS changes in order to increase NRC efficiency and reduce unnecessary regulatory burden. The NRC role in maintaining plant safety is achieved by the technical review of proposed changes to the STS as well as plant-specific applications to adopt NRC-accepted changes to the STS.

3.0 TECHNICAL EVALUATION

The WOG stated that the approach used in WCAP-15376-P, Rev. 0, to justify the proposed revisions to CTs and STIs for the RTS and ESFAS, is consistent with the guidance outlined in RGs 1.174 and 1.177. The WOG further stated that the increase in surveillance intervals will reduce the required testing on the reactor protection system components without significantly reducing their reliability, and reduce the potential for reactor trips and actuation of engineered safety features associated with testing of these components. In addition, the WOG stated that the CT extensions for the reactor trip breakers will provide the licensees additional time to complete test and maintenance activities while at power, potentially reducing the number of forced outages related to compliance with reactor trip breakers and provide consistency with the CT previously approved by the staff for the logic cabinets under WCAP-14333-P. The staff used a three-tiered approach in its evaluation of the risk associated with the proposed TS changes in RPS and ESFAS surveillance test, completion, and bypass times. The review approach is consistent with the guidance in RG 1.177. The first tier evaluates the PRA model and includes the RTS and ESFAS unavailability analyses and risk analyses that support the risk impact assessment. The second tier addresses the need to preclude potentially high risk configurations should additional equipment outages occur during the proposed CT period. The third tier evaluates the licensee's configuration risk management program to ensure that equipment outage due to maintenance, testing, or random failure immediately prior to or during the proposed CT will be appropriately assessed from a risk perspective.

3.1 Tier 1: PRA Capability and Insights

Westinghouse used traditional PRA methodology to evaluate the requested TS changes. To support this assessment, two aspects had to be considered: (1) an evaluation of the PRA model and application to the proposed changes, and (2) an evaluation of PRA results and insights stemming from the application. The staff concluded that Westinghouse's PRA is valid for assessing the proposed TS changes and identifies the impact of the TS change on plant risk. The WOG stated that the unavailability data used in the model came from several sources including previous RTS and ESFAS studies, WCAP-10271 and WCAP-14333-P. The WOG also used data from NUREG/CR-5500, Vol. 2, "Reliability Study: Westinghouse Reactor Protection System, 1984-1995."

The staff's review concerned itself with the development of the PRA model and its applicability in the evaluation of plant risk based on the proposed changes. Westinghouse used component failure probabilities derived from NUREG/CR-5500, Vol. 2, and additional component failure probabilities from WCAP-10271-P, and WCAP-14333-P, both of which were previously approved by the staff. The WOG also surveyed various plants to obtain operational data for SSPS safeguard driver cards and master relays for both the relay and SSPS-based RPS. As a result, the failure probabilities used in WCAP-15376-P, Rev. 0, were developed using plant operating experience rather than the generic reliability factors used in WCAP-10271-P and WCAP-14333-P.

The plant survey data indicated that the failure probability of the master relay for the relay protection system was higher than the SSPS. Based on this, the WOG chose not to propose extending STIs for the master relays associated with a relay protection system, but maintain surveillance testing at current intervals.

3.1.1 Evaluation of PRA Model and Its Application to the CT Extension

WCAP-15376-P, Rev. 0, used the Vogtle PRA model to evaluate the impact on risk of the proposed changes. The Vogtle PRA was developed in response to Generic Letter (GL) 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities." The staff concluded that the Vogtle Individual Plant Examination (IPE) met the intent of GL 88-20. The Vogtle PRA model was previously utilized in WCAP-14333-P to provide the basis tor extending CTs for the RPS. Since the requested surveillance interval and CT requests in WCAP-15376-P, Rev. 0, are similar in scope to those requested by WCAP-14333-P, the WOG utilized the same model for WCAP-15376-P, Rev. 0. WCAP-15376-P, Rev. 0, provides various insights as to the appropriateness of the Vogtle model in support of the proposed TS changes stating that the model provides sufficient detail to perform the analysis, the Vogtle model includes anticipated transient without scram (ATWS), and the Vogtle model allows operator action to be credited.

The model used in WCAP-14333-P is not identical to the model used for WCAP-15376-P, Rev. 0. Changes were made to the model including the replacement of WCAP-10271 data with proprietary plant data collected by Westinghouse and the use of NUREG/CR-5500 failure data. Logic changes included the modeling of the SSPS at the card level instead of the component level as was done in WCAP-10271-P and WCAP-14333-P. The staff did not review the quality of the proprietary data in detail, but the use of more recent generic data, including Westinghouse specific data, should result in improved assessment of the unavailability estimates. Based on the use of the same model as a previous evaluation (with updated data), the staff finds that the quality of the PRA is sufficient for the evaluation of the proposed changes. However, the analysis did not report uncertainty bounds for the proprietary data estimates which may have an influence on plant-specific results. Based on the above, a plant-specific analysis should consider the uncertainty in the data consistent with RG 1.174 and RG 1.177 guidance to ensure that the conclusions of WCAP-15376-P, Rev. 0, remain valid for the plant-specific case.

The analysis performed in WCAP-15376-P, Rev. 0, included fault trees of representative RTS signals and ESFAS actuation for the SSPS (including 2 of 3 and 3 of 4 logic) and relay protection system (including 2 of 3 and 3 of 4 logic). WCAP-15376-P, Rev. 0, concluded that the SSPS unavailability estimates bound the relay protection system unavailability estimates. As a result, the estimates for the SSPS were used in the analysis of the Vogtle PRA in estimating the CDF and LERF for the current TS case and the proposed TS surveillance intervals and CTs.

To evaluate the results presented in WCAP-15376-P, Rev. 0, an independent model was developed for selected RPS signals. In response to the staff's request, the WOG provided additional data to quantify the base case. The generic data that was used in the model was verified. Revised component unavailabilities and failure probabilities were used to determine new signal unavailabilities. The proposed TS amendment request changes were individually evaluated using the same cases as WCAP-15376-P, Rev. 0. The "combined cases" representing the proposed TS changes were evaluated for the bounding SSPS plant. The results were consistent with those reported in WCAP-15376-P, Rev. 0.

3.1.2 Change in CDF

The unavailability analysis did not model or evaluate all RTS and ESFAS signals in the fault tree analysis. Consistent with WCAP-14333-P, only representative signals were evaluated in detail. The risk analysis used the results from the unavailability analysis to determine the impact that the proposed changes had on the availability of the RPS. The base case was represented by the CTs, bypass times, and STIs previously approved in WCAP-14333-P. The representative signals included safety injection, auxiliary feedwater, reactor trip initiation - pressurizer high, and reactor trip on pressurizer high or over temperature delta T. The availability of diverse signals, including operator action if the automatic actuation fails, were considered in the WCAP-15376-P, Rev. 0 analysis. The representative model selected was based on the Vogtle plant which is a variation on the model used for the analysis in WCAP-14333-P and included fault trees for both RPS and ESFAS. The fault trees were modeled in sufficient detail to allow the CTs and STI to be varied for the components included in WCAP-15376, Rev. 0. The base case model was quantified according to the approved changes in WCAP-14333-P and includes updated component data using Westinghouse proprietary and generic plant failure rates. The WCAP-15376-P, Rev. 0 analysis did not credit any potential trip reduction over that taken by the previous WCAP-10271-P study. WCAP-15376-P, Rev. 0 took credit for decreased unavailability due to reduced test frequency and accounted for the increase in fault exposure time when increasing the STI intervals.

The baseline value for CDF was calculated to be 5.05E-5/r-yr for both 2/4 logic and 2/3 logic RPS. The topical report then presented a series of TS sensitivity cases with each case including RPS components slated for STI or CT modification and the CDF and LERF calculated and compared to the acceptance guidelines defined by RG 1.174 and RG 1.177. For the proposed TS changes, the CDF increased to 5.13E-5/r-yr and 5.14E-5/r-yr for 2/4 and 2/3 logic signals, respectively. RG 1.174 acceptance guidelines state that when the calculated increase in CDF is less than 10E-6/r-yr, the change will be considered regardless of whether there is calculation of total CDF as long as there is no indication that the total CDF is not considerably higher than 10E-4/r-yr. For increases in CDF in the range of 10E-6/r-yr to 1E-5/r-yr, applications will be considered only if it can be reasonably shown that the total CDF is less than 10E-4/r-yr. Therefore, the proposed CT and STI changes are acceptable to the staff with respect to ΔCDF.

The WOG also evaluated the LERF for the RTBs, master relays, logic cabinets, and analog channels. Based on the values presented in WCAP-15376-P, Rev. 0, the change in LERF when implementing proposed TS changes is 3.09E-8/r-yr and 5.68E-8/r-yr for 2/4 and 2/3 logic signals, respectively. Both values are within the 10E-7/r-yr of acceptance guidelines stated in RG 1.174 and are acceptable to the staff.

These values are based on the assumption that the only contributions to LERF would come from containment bypass events and core damage events with the containment not isolated. The contributions from containment failure events are not considered in WCAP-15376-P, Rev. 0 based on the Vogtle PRA and the assumption that Vogtle is representative of all Westinghouse plants. There may be exceptions to this assumption, including Westinghouse plants with an ice condenser containment. Studies have shown that ice condenser plants can be substantially more sensitive to early containment failure than pressurized water reactors (PWRs) with a large dry or sub-atmospheric containment. For example, in an ice condenser plant with a higher station blackout frequency, early containment failure may be important. A plant-specific assessment of containment failures should be performed for all plants referencing this topical report to determine whether there are any impacts on the proposed TS changes. WCAP-15376-P, Rev. 0 also states that if the ICCDP value meets the RG criterion then the ICLERP value would also meet the associated guideline value in the RG. These assumptions may not be the case for specific plants in that the plant differences may affect the results when compared to the reference plant. Therefore, for plant-specific cases, a licensee will need to confirm that both the ICCDP and ICLERP values for the proposed change meet the guidance outlined in RG. 1.177 and RG 1.174.

3.1.3 Single CT Risk

The base case model was also re-quantified to evaluate the proposed CT for the RTB. The model assumed one RTB was out-of-service with the associated bypass breaker available. The operable RTB and the in-service bypass breaker provide the reactor trip. In this arrangement both breakers are controlled by the logic cabinet associated with the operable breaker. The proposed change revises the RTB bypass time to 4 hours to be consistent with the logic cabinets and the CT for the RTBs also is increased to 24 hours to match the logic cabinet CT. The WOG estimated a conditional CDF of 7.07E-5/r-yr for this configuration and estimated the ICCDP to be 6.9E-8/r-yr. The value for the ICCDP is within the RG 1.177 acceptance guideline of less than 5.0E-7/r-yr.

However, WCAP-14333-P accepted the case where a logic cabinet and associated RTB may be tested concurrently, provided that the RTB is bypassed for a period of time equivalent to the bypass time for the logic cabinet. This testing arrangement causes the respective RPS train to be inoperable when in a test or maintenance condition. Because WCAP-14333-P approved concurrent testing of the RTB and associate logic cabinet, the staff questioned modeling the proposed bypass time and CT with only the RTB out of service. The WOG's response indicated that the WOG's intent is to remove both the RTB and its associated logic cabinet from service during surveillance testing. With the more limiting configuration of having both the RTB and the associated logic cabinet out-of-service, the conditional CDF was calculated to be 1.45E-4/r-yr with an ICCDP risk of 3.2E-7/r-yr. The risk of this configuration is substantially higher (by a factor of 5) than when only an RTB is inoperable, but is more representative of the LCO configuration to be implemented during surveillance testing. However, the revised ICCDP still remains bounded by the RG 1.177 acceptance guideline of 5.0E-7/r-yr. The change in CDF also meets RG 1.174 acceptance guidelines (see Section 3.1.2). A licensee implementing this surveillance configuration may require additional plant-specific Tier 1 and Tier 2 analyses to confirm that the generic analysis for WCAP-15376-P, Rev. 0, remains bounding for the plant-specific case.

3.1.4 Shutdown Risk and Transition Risk

WCAP-15376-P, Rev. 0, states that one advantage for extending the CT for the RTBs is that the exposure to transition risk would be decreased since the extended CT would limit the transition to lower modes should the present RTB CT be exceeded. The WOG also claimed that the transition risk would be comparable to the risk increase caused by the requested CT extension for the RTBs.

The staff finds that the evaluation of transition risk would only occur when unscheduled corrective maintenance cannot be completed within the allotted time specified by the TS. In cases where a failure condition is observed during an RTB surveillance test, the decision to repair at power or perform a mode change should consider the transition risk. However, it has limited applicability to the proposed surveillance AOT extension request. The analysis presented in WCAP-15376-P, Rev. 0 for maintenance risk and transition risk assumes only that the RTB is out-of-service and not a complete train of RPS.

3.1.5 Common Cause Failures

The WOG used the Multiple Greek Letter Method (MGL) for the analog channels and the Bete Factor approach for the RTB, logic cabinet, master and slave relays. The analysis in WCAP-15376-P, Rev. 0 did not distinguish between components being down due to failure (corrective maintenance) when evaluating common cause failures. In response to the request for additional information (RAI), the WOG provided an estimate of the single CT risk for both corrective maintenance and preventive maintenance. Based on the WOG's results, the single CT risk did not change for corrective or preventive maintenance. The WOG stated that a significant change in risk is not observed since the reactor trip signal is dominated by the failure of the logic cabinet as opposed to the failure of both RTBs. These results are only applicable for surveillance performed with both the RTB and logic cabinet out-of-service. In this case, the remaining operable logic cabinet failures appear to dominate the failure of the RPS signal since the logic cabinet supports both RPS and ESFAS functions. For cases where only an RTB is removed, then the unaffected RTB may become risk significant.

3.1.6 Application of Vogtle Model to the Plant-Specific Case

The applicability of the Vogtle PRA model to other Westinghouse plants was evaluated by the staff. WCAP-15376-P, Rev. 0 states that RPS/ESFAS functions are similar in response across all Westinghouse plants for initiating events. Additionally, the safety functions challenged in response to initiating events and the associated actuation signals generated are also similar and procedures provide for operator action to back up automatic initiation of safety systems.

Although the staff recognizes the similarity between plant RPS and ESFAS systems, design, function, and initiating event frequency, the unavailability of the RPS shows a wide range of estimates. These differences may result from varying model assumptions (including operator action), the generic or plant-specific data used, actual design differences or variations in plant-specific equipment performance (master relays for example). Another example identified in the review was what appeared to be a substantial variability in the contribution to core damage due to ATWS events. The WOG provided a summary of ATWS contributions for various plants. Based on the data provided, the contribution to core damage frequency for ATWS events at Westinghouse plants varied from less than 0.1 to approximately 20 percent with the WCAP-15376-P, Rev. 0 Vogtle model showing a contribution of 2.1 percent. Another factor that may contribute to the variability in plant risk is the assumption of operator action in the PRA model. The analysis in WCAP-15376-P, Rev. 0 is centered on the automatic functions performed by the RPS with operator action credited in the topical report. Based on the above, a licensee incorporating WCAP-15376-P, Rev. 0 is expected to confirm the applicability of the topical report to their plant and to address any design or performance differences that may affect the proposed CT and STI assumptions. Additionally, to ensure consistency with the reference plant, the model assumptions for human reliability in the topical report should be confirmed to be applicable to the plant-specific case. In the Tier 1 evaluation for WCAP-15376-P, Rev. 0, the WOG evaluated the impact of the proposed changes on CDF, ICCDP, LERF, and ICLERP. The staff found that the use of the Vogtle PRA as a representative model was reasonable for assessing the proposed TS changes and that the risk impact was within the guidelines stated for ΔCDF, ICCDP, ΔLERF, and ICLERP in RG 1.174 and RG 1.177. However, the applicability of the generic model must be confirmed when applying the results of WCAP-15376-P, Rev. 0 to a plant-specific license amendment.

The WOG stated that although the WCAP-15376-P, Rev. 0 analysis and the results obtained were only for analog systems, the results are also applicable to digital systems based on previous applications of WOG TOP with Eagle 21 systems. The staff notes that the Eagle 21 system provides for improved on-line monitoring and based on previous evaluations has similar unavailabilities to an analog RTS. However, the Eagle 21 upgrade only replaced the channel process logic modules of the RTS with an integrated microprocessor-based module and thus was limited in scope. Digital upgrades with increased scope, integration, and architectural differences may affect plant risk and therefore surveillance requirements. Therefore, the staff finds that the generic applicability of WCAP-15376-P, Rev. 0 to future digital systems is not clear and should be considered on a plant-specific basis.

3.2 Impact on Defense-In-Depth and Safety Margins

The traditional engineering considerations need to be addressed. These include defense-in-depth and safety margins. The fundamental safety principles on which the plant design is based cannot be compromised. Design basis accidents are used to develop the plant design. These are a combination of postulated challenges and failure events that are used in the plant design to demonstrate safe plant response. Defense-in-depth, the single failure criterion, and adequate safety margins may be impacted by the proposed change and consideration needs to be given to these elements.

3.2.1 Impact on Defense-In-Depth

The proposed STI changes to the RTS and ESFAS and the proposed change to the RTB CT have only a small calculated impact on CDF and LERF. The CT and STI changes to the RTB only impact CDF and have no impact on containment integrity. The STI changes to the analog channels, logic cabinets, and master relays have small calculated impacts on both CDF and LERF. These changes do not degrade core damage prevention at the expense of containment integrity, nor do these changes degrade containment integrity at the expense of core damage prevention. The balance between prevention of core damage and prevention of containment failure is maintained. Consequence mitigation remains unaffected by the proposed changes. Furthermore, no new accident or transients are introduced with the proposed changes, and the likelihood of an accident or transient is not impacted. No new activities on the RPS will be performed at power that could lead to potentially new transient events. Conversely, the increase in STIs could potentially lead to a reduction in the likelihood of a test induced transient or accident.

The plant design will not be changed with these proposed changes. All safety systems, including the RPS, will still function in the same manner with the same signals available to trip the reactor and initiate ESF functions, and there will be no additional reliance on additional systems, procedures, or operator actions. The calculated risk increase for these changes is very small and additional control processes are not required to be put into place to compensate for any risk increase.

There is no impact on the redundancy, independence, or diversity of the RPS or the ability of the plant to respond to events with diverse systems. The RPS is a diverse and redundant system and will remain so. There will be no change to the signals available to trip the reactor or initiate ESF functions. The RPS is a reliable system and is backed up by the plant operators who will still be available to perform actions in the occurrence of RPS failure. In addition, the RTS is backed up by ATWS mitigating system actuation circuitry (AMSAC) signal to start auxiliary feedwater and trip the turbine in conjunction with RCS pressure mitigation via the pressurizer safety valves and relief valves. The proposed changes have no impact on this alternate approach to ATWS mitigation.

Defense against common cause failures was reviewed by the staff. The extensions requested are not sufficiently long to expect new common cause failure mechanisms to arise. In addition, the operating environment for these components remains the same, so new common cause failure modes are not anticipated. Also, backup systems and operator actions are not impacted by these changes; and there are no common cause links between the RPS and these backup options. Furthermore, the RTB CT and bypass time increases are not requested to perform additional tests and routine maintenance activities while at power. Such activities will continue to be completed as currently required. Therefore, no new potential common cause failure mechanisms have been introduced.

No new operator actions related to the STI extension or the CT extension are required. No additional operating, maintenance, or test procedures have been introduced or modified due to these changes, and no new at-power tests or maintenance activities are expected to occur as a result of these changes. The plant will continue to be operated and maintained as before. With the CT increase, the plant can be maintained at power longer to complete repair activities on the RTBs. With the STI increase, fewer surveillance tests will need to be completed at-power which will reduce the potential for test induced reactor trips and safety system actuations.

3.2.2 Impact on Safety Margins

The safety analysis acceptance criteria as stated in the Final Safety Analysis Report is not impacted by these changes. Redundant RPS trains will be maintained. Diversity with regard to signals to provide reactor trip and actuation of engineered safety features will also be maintained. The proposed changes will not allow plant operation in a configuration outside the design basis. All signals credited as primary or secondary and all operator actions credited in the accident analysis will remain the same.

3.3 Tier 2: Avoidance of Risk-Significant Plant Configuration

The licensee should provide reasonable assurance that risk significant plant equipment outage configurations will not occur when specific plant equipment is out-of-service in accordance with the proposed TS change. The WOG identified the following restrictions on equipment removal when an RTB is out of service:

1. With an RTB out-of-service, systems designed to mitigate an ATWS event should be available. Also identified were RCS pressure relief, auxiliary feedwater flow, AMSAC, and turbine trip. Based on the above, WCAP-15376-P, Rev. 0 stated that activities that degrade the availability of auxiliary feedwater, RCS pressure relief, AMSAC, or turbine trip should not be scheduled when an RTB is out-of-service.

2. Because there is increased dependence on the available reactor trip train when one logic cabinet is removed from service, activities that could degrade other components of the RPS including master relays, slave relays, and analog channels should not be scheduled concurrently with a logic cabinet out of service.

3. WCAP-15376-P, Rev. 0 also noted that activities on electrical support systems for the equipment identified should not be scheduled during RTB maintenance.

Therefore, a licensee should evaluate the need for and develop the necessary restriction on concurrent equipment outages when entering proposed RTB CT to avoid potential risk significant configurations.

3.4 Tier 3: Risk-Informed Plant Configuration Control and Management

The WOG did not provide detailed information on the Tier 3, 10-CFR 50.65(a)(4) CRMP due to the plant-specific nature of the information required. Each licensee should develop a program that ensures that the risk impact of out-of-service equipment is appropriately evaluated prior to performing the maintenance activity. The program should be able to uncover risk significant plant outage configuration and should include such factors as equipment unavailability, operational activities, and weather conditions. The Tier 3 program provides additional assurance over the Tier 2 program by identifying risk significant configurations that may be encountered over extended periods of plant operation. The CRMP program referenced by RG 1.174 may be implemented by a licensee through the maintenance rule (10 CFR 50.65(a)(4)), which requires that the licensee before performing maintenance activities, shall assess and manage the increase in risk that may result from the proposed maintenance activity.

3.5 TSTF-411, Rev. 1 Evaluation

The proposed NUREG-1431 changes revise TSs and Bases for Reactor Protection System Instrumentation (3.3.1), Engineered Safety Feature System Instrumentation (3.3.2), Containment Purge and Exhaust Isolation Instrumentation (3.3.6), Control Room Emergency Filtration System Actuation Instrumentation (3.3.7), and Boron Dilution Protection System Instrumentation (3.3.9).

Specifically, the RTB bypass test time allowance changes to 4 hours from 2 hours; the CT allowance changes to 24 hours from 1 hour; and the surveillance frequency changes to 4 months from 2 months in Specification 3.3.1 for both SSPS and RPS designs. The surveillance frequencies for logic cabinets changes to 6 months from 2 months for SSPS plants and to 6 months from 1 month for RPS plants. Master relays changes to 6 months from 2 months for SSPS plants, and analog channels changes to 6 months from 3 months in Specifications 3.3.1, 3.3.2, 3.3.6, 3.3.7 and 3.3.9. In addition, changes were made to TS 3.3.1 and 3.3.2 Bases. Appropriate to WCAP-13632 and WCAP-14036, references were added to the Bases discussions in accordance with approved TSTF-111, Rev. 6. Also, references in Surveillance Requirement (SR) 3.3.7.3 and SR 3.3.9.3 were corrected to reflect an appropriate citation.

The NRC staff reviewed the proposed generic relaxations contained in TSTF-411, Rev. 1 and found them acceptable because they are consistent with current licensing practices and the Commission's regulations.

3.5.1 Relaxation of Completion Time

Upon discovery of a failure to meet an LCO, TS specify times for completing Required Actions of the associated TS conditions. Required Actions establish remedial measures that must be taken within specified completion times. These times define limits during which operation in a degraded condition is permitted. Incorporating required action and completion time extensions is acceptable because these times take into account the operability status of the redundant systems of TS required features, the capacity and capability of remaining features, a reasonable time for repairs or replacement of required features, and the low probability of a design basis accident (DBA) occurring during the repair period.

The TSTF-411, Rev. 1 proposed changes reduce required testing on the reactor protection system components and reduce the potential for reactor trips and actuation of engineered safety features associated with the testing of these components. The required action CT extension for the RTBs will provide additional time to complete test and maintenance activities while at power, potentially reducing the number of forced outages related to compliance with RTB CTs, and provide consistency with the CTs for the testing of RPS logic cabinets.

3.5.2 Relaxation of Surveillance Requirement

TS require maintaining the LCO equipment operable by meeting the SRs in accordance with the specified SR Frequency. This requires conducting tests to demonstrate equipment is operable, or that LCO parameters are within specified limits. When the test acceptance criteria and any specified conditions for the conduct of the test are met, the equipment is deemed operable. TSTF-411, Rev. 1 includes changes related to relaxation of STS SR frequencies. Relaxing the SR frequency provides operational flexibility consistent with the objective of the STS without reducing confidence that the equipment is operable. The changes are acceptable because appropriate testing standards are retained for determining that the LCO-required features are operable. These relaxations of SRs optimize test requirements for the affected safety systems and increase operational flexibility.

4.0 CONCLUSION

The staff review of the proposed changes finds that WCAP-15376-P, Rev. 0 is consistent with acceptance guidelines of RG 1.174, RG 1.177, and staff guidance as outlined in NUREG-0800, "Standard Review Plan." From traditional engineering insights, including the defense-in-depth philosophy and the safety margins, the staff finds that the proposed changes have no impact on the defense-in-depth philosophy and safety margin. The staff further determines that the implementation of the proposed changes for CT and STI for RTS and ESFAS, including signals processed through either the relay or SSPS, should result in only a minimal quantitative impact on plant risk.

The staff also concludes that TSTF-411, Rev. 1 proposed generic TS changes are consistent with the approved allowances for RTB testing with an instrument channel in bypass, for RTB repair completion times and for surveillance frequency changes to logic cabinets for SSPS and relay protection system plant designs, for master relays for SSPS plants and analog channels accepted by the staff based on WCAP-15376-P, Rev. 0. In addition, the proposed TS Bases provide an adequate basis or reason for the STS changes and editorial guidelines of the STS "Writer's Guide" were followed for preparing STS changes. Thus, TSTF-411, Rev. 1 preserves the human factors principles used throughout the development of NUREG-1431 and can be appropriately applied to licensee specific TS changes.

5.0 CONDITIONS AND LIMITATIONS

Although the engineering consideration and PRA insights support the proposed changes, the applicability of WCAP-15376-P, Rev. 0 on a plant-specific basis needs to be confirmed by providing the following information:

1. A licensee is expected to confirm the applicability of the topical report to their plant, and to perform a plant-specific assessment of containment failures and address any design or performance differences that may affect the proposed changes.

2. Address the Tier 2 and Tier 3 analyses including risk significant configuration insights and confirm that these insights are incorporated into the plant-specific configuration risk management program.

3. The risk impact of concurrent testing of one logic cabinet and associated reactor trip breaker needs to be evaluated on a plant-specific basis to ensure conformance with the WCAP-15376-P, Rev. 0 evaluation, and RGs 1.174 and 1.177 guidance.

4. To ensure consistency with the reference plant, the model assumptions for human reliability in WCAP-15376-P, Rev. 0 should be confirmed to be applicable to the plant-specific configuration.

5. For future digital upgrades with increased scope, integration and architectural differences beyond that of Eagle 21, the staff finds the generic applicability of WCAP-15376-P, Rev. 0 to future digital systems not clear and should be considered on a plant-specific basis.

Principal Contributors: Cliff Doutt
Sang Rhow
Carl Schulten

Date: December 20, 2002

NRC Approval of TSTF-411, Rev. 1
"Surveillance Test Interval Extensions for
Components of the Reactor Protection System"

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

August 30, 2002

Mr. Anthony Pietrangelo
Nuclear Energy Institute
1776 I Street, N. W.
Suite 400
Washington, DC 20006-3708

Dear Mr. Pietrangelo:

The Nuclear Regulatory Commission has completed its review of the Nuclear Energy Institute Technical Specification Change Traveler, TSTF-411, Rev. 1" Surveillance Test Interval Extensions for Components of the Reactor Protection System" proposed changes to NUREG-1431, Rev. 2, "Standard Technical Specifications Westinghouse Plants." The staff finds the proposed changes acceptable without modification. Accordingly, the staff will instruct Westinghouse to include TSTF-411, Rev. 1 with publication of the approved version of WCAP-15376-P. The safety evaluation approving this WCAP will also contain the basis for approving the TSTF. Individual licensees may then propose to adopt the approved TS during a conversion to the STS or as a separate license amendment application for WCAP-15376-P.

Please contact me at (301) 415-1161 or e-mail wdb@nrc.gov if you have any questions or need further information on these proposed changes.

Sincerely,

William D. Beckner, Program Director
Operating Reactor Improvements Program
Division of Regulatory Improvement Programs
Office of Nuclear Reactor Regulation

cc: J. Arbuckle, BWROG
D. Bice, CEOG
N. Clarkson, BWOG
S. Wideman, WOG
D. Hoffman, EXCEL

WESTINGHOUSE NON-PROPRIETARY CLASS 3

WCAP-15377-NP-A
Revision 1

Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times

D. V. Lockridge
G. R. Andre
R. L. Haessler
J. D. Andrachek
R. M. Span

March 2003

This work was performed under WOG Shop Orders MUHP-3045 and MUHP-3046

Westinghouse Electric Company LLC
Nuclear Services Business Unit
P.O. Box 355
Pittsburgh, PA 15230-0355

WESTINGHOUSE COPYRIGHT NOTICE AND LIABILITY STATEMENT

This report bears a Westinghouse copyright notice. You as a member of the Westinghouse Owners Group are permitted to make the number of copies of the information contained in this report which are necessary for your internal use in connection with your implementation of the report results for your plant(s) in your normal conduct of business. Should implementation of this report involve a third party, you are permitted to make the number of copies of the information contained in this report which are necessary for the third party's use in supporting your implementation at your plant(s) in your normal conduct of business, recognizing that the appropriate agreements must be in place to protect the proprietary information for the proprietary version of the report. All copies made by you must include the copyright notice in all instances and the proprietary notice if the original was identified as proprietary.

This report was prepared by Westinghouse Electric Company LLC as an account of work sponsored by the Westinghouse Owners Group (WOG). Neither the WOG, any member of the WOG, Westinghouse Electric Company LLC, nor any person acting on behalf of any of them:

- Makes any warranty or representation whatsoever, express or implied, (i) with respect to the use of any information, apparatus, method, process, or similar item disclosed in this report, including merchantability and fitness for a particular purpose, (ii) that such use does not infringe on or interfere with privately owned rights, including any party's intellectual property, or (iii) that this report is suitable to any particular user's circumstance; or

- Assumes responsibility for any damages or other liability whatsoever (including any consequential damages, even if the WOG or any WOG representative has been advised of the possibility of such damages) resulting from any selection or use of this report or any information apparatus, method, process, or similar item disclosed in this report.

FOREWORD

This document contains Westinghouse Electric Company proprietary information and data which has been identified by brackets. Codmg associated with the brackets sets forth the basis on which the information is considered proprietary. These codes are listed with their meanings in WCAP-7211.

The proprietary information and data contained in this report were obtained at considerable Westinghouse expense and its release could seriously affect our competitive position. This information is to be withheld from public disclosure in accordance with the Rules of Practice 10 CFR 2.790 and the information presented herein be safeguarded in accordance with 10 CFR 2.903. Withholding of this information does not adversely affect the public interest.

This information has been provided for your internal use only and should not be released to persons or organizations outside the Directorate of Regulation and the ACRS without the express written approval of Westinghouse Electric Company. Should it become necessary to release this information to such persons as part of the review procedure, please contact Westinghouse Electric Company, which will make necessary the arrangements required to protect the Company's proprietary interests.

The proprietary information is deleted in the unclassified version of this report (WCAP-15377).

TABLE OF CONTENTS

TABLE OF CONTENTS (cont'd.)

LIST OF TABLES

LIST OF TABLES (cont'd.)

LIST OF FIGURES

ACRONYMS

AC	Alternating Current
AFW	Auxiliary Feedwater
AFWPS	Auxiliary Feedwater Pump Start
AMSAC	ATWS Mitigating System Actuation Circuitry
AOT	Allowed Outage Time
ATWS	Anticipated Transient Without Scram
BDPS	Boron Dilution Protection System
CCF	Common Cause Failure
CDF	Core Damage Frequency
COT	Channel Operability Test
CT	Completion Time
DC	Direct Current
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FW	Feedwater
ICCDP	Incremental Conditional Core Damage Probability
ICLERP	Incremental Conditional Large Early Release Probability
IPE	Individual Plant Examination
LER	Licensee Event Report
LERF	Large Early Release Frequency
LCO	Limiting Condition for Operation
LOCA	Loss of Coolant Accident
NEAP	Not Evaluated At-Power
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
OA	Operator Action
PORV	Power Operated Relief Valve
PWR	Pressurized Water Reactor
RCS	Reactor Coolant System
RPS	Reactor Protection System
RT	Reactor Trip
RTB	Reactor Trip Breaker
RTS	Reactor Trip System
RWST	Refueling Water Storage Tank
SI	Safety Injection
SSPS	Solid State Protection System
STI	Surveillance Test Interval
T	Temperature
TOP	Technical Specification Optimization Program
WOG	Westinghouse Owners Group

ABSTRACT

The objective of this program is to provide the justification for the following changes to the Technical Specifications for the Reactor Trip System (RTS) Instrumentation (3.3.1) and Engineered Safety Features Actuation System (ESFAS) Instrumentation (3.3.2):

1. Increase the Completion Time (CT) and the bypass test time for the reactor trip breakers.

2. Increase the Surveillance Test Intervals (STI) for the reactor trip breakers, master relays, logic cabinets, and analog channels.

This evaluation considers both the Solid State Protection System and the Relay Protection System.

Depending on the plant protection system design, some of the actuation logic and master relays associated with the Containment Purge and Exhaust Isolation Instrumentation (3.3.6) and CREFS Actuation Instrumentation (3.3.7) Technical Specifications may be processed through the Relay or Solid State Protection System. Since the STIs for the actuation logic and master relays of the ESFAS Instrumentation were justified to be relaxed in this report, these STI relaxations are also applicable to the actuation logic and master relays for all signals processed through the Relay or Solid State Protection System.

The STI for the source range neutron flux Channel Operational Test (COT) in the RTS Instrumentation (3.3.1) Technical Specification was justified to be relaxed in this report. Since this source range neutron flux channel is also used for the BDPS in Technical Specification 3.3.9, the STI relaxation is also applicable to that STI.

The approach used in this program is consistent with the Nuclear Regulatory Commission's (NRC) approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the current licensing basis as presented in Regulatory Guides 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis" (Reference 1) and 1.177, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications", (Reference 2). The approach addresses the impact on defense-in-depth and the impact on safety margins, as well as an evaluation of the impact on risk.

The Surveillance Test Interval (STI) changes will reduce the required testing on the reactor protection system components without significantly impacting its reliability, and reduce the potential for reactor trips and actuation of engineered safety features associated with the testing of these components. The Completion Time (CT) extensions for the reactor trip breakers will provide the utilities additional time to complete test and maintenance activities while at power, potentially reducing the number of forced outages related to compliance with reactor trip breaker CTs, and provide consistency with the CTs for the logic cabinets.

1.0 INTRODUCTION

The purpose of this program is to provide the technical justification for extending the surveillance test intervals (STIs) for components of the reactor protection system. The components specifically included are the analog channels, logic cabinets, master relays, and reactor trip breakers. This program also provides the technical justification for extending the reactor trip breaker (RTB) completion time (allowed outage time) for one RTB inoperable to 24 hours and the bypass time for a RTB to 4 hours. This completion time (CT) and bypass time are consistent with the CT and bypass time for the logic cabinets. This evaluation considers both the solid state protection system and the relay protection systems. Extension of the STIs for slave relays are not included in this assessment, since they were previously addressed in other WOG programs.

Depending on the plant protection system design, some of the actuation logic and master relays associated with the Containment Purge and Exhaust Isolation Instrumentation (3.3.6) and CREFS Actuation Instrumentation (3.3.7) Technical Specifications may be processed through the Relay or Solid State Protection System. Since the STIs for the actuation logic and master relays of the ESFAS Instrumentation were justified to be relaxed in this report, these STI relaxations are also applicable to the actuation logic and master relays for all signals processed through the Relay or Solid State Protection System.

The STI for the source range neutron flux Channel Operational Test (COT) in the RTS Instrumentation (3.3.1) Technical Specification was justified to be relaxed in this report. Since this source range neutron flux channel is also used for the BDPS in Technical Specification 3.3.9, the STI relaxation is also applicable to that STI.

The approach used in this program is consistent with the Nuclear Regulatory Commission's (NRC) approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the current licensing basis as presented in Regulatory Guides 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis" (Reference 1) and 1.177, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications", (Reference 2). The approach addresses, as documented in this report, the impact on defense-in-depth and the impact on safety margins, as well as an evaluation of the impact on risk. The risk evaluation considers the three-tiered approach as presented by the NRC in Reference 2 for the extension to the RTB CT. Tier 1, *PRA Capability and Insights*, assesses the impact of the proposed CT (AOT) change on core damage frequency (CDF), incremental conditional core damage probability (ICCDP), large early release frequency (LERF), and incremental conditional large early release probability (ICLERP). Tier 2, *Avoidance of Risk-Significant Plant Configurations*, considers potential risk-significant plant operating configurations. Tier 3, *Risk-Informed Plant Configuration Control and Management*, will be addressed on a plant specific basis when the Technical Specification Completion Time change is implemented by each utility.

The STI changes will reduce the required testing on the reactor protection system components, a highly reliable system, without impacting its reliability. The CT extensions for the RTBs will provide the utilities additional time to complete test and maintenance activities while at power and provide consistency with the CTs for the logic cabinets.

The Westinghouse Owners Group is evaluating these changes as part of an overall program addressing Technical Specification improvements for the RPS which includes reactor trip signals and engineered safety features actuation signals. The initial studies (References 3, 4, 5, 6) evaluated changes to AOTs, bypass time, and STIs to the analog channels, logic cabinets, master relays, slave relays, and reactor trip breakers of the RPS. The previously approved changes to these parameters are summarized in Table 1.1 and 1.2 for the SSPS and the relay protection systems.

Table 1.1 Summary of STI and AOT Changes for the Various WOG Instrumentation Technical Specification Improvement Programs (Solid State Protection System)

Component	Pre-TOP	WCAP-10271 (TOP)	WCAP-14333
Analog Channels			
- CT	1 hour	6 hours	72 hours
- Bypass Time	2 hours	4 hours	12 hours
- COT[2] STI	1 month	3 months	3 months
- Calibration Interval	NEAP[1]	NEAP[1]	18 months
- Calibration Time	NEAP[1]	NEAP[1]	4 hours
Logic Cabinet			
- CT	2 hours	6 hours	24 hours
- Bypass Time	1.5 hours	4 hours	4 hours
- STI	2 months	2 months	2 months
Master Relay			
- CT	2 hours	6 hours	24 hours
- Bypass Time	1.5 hours	4 hours	4 hours
- STI	2 months	2 months	2 months
Slave Relay			
- CT	2 hours	6 hours	24 hours
- Bypass Time	4 hours	4 hours	4 hours
- STI	3 months	3 months	3 months
Reactor Trip Breakers			
- CT	6 hours	6 hours	6 hours
- Bypass Time	2 hours	2 hours	2 hours
- STI	2 months	2 months	2 months

Notes

1) NEAP - Not Evaluated At-Power, previously this activity has typically been done while shutdown.

2) COT - Channel Operational Test (bypass or test time)

Table 1.2 Summary of STI and AOT Changes for the Various WOG Instrumentation Technical Specification Improvement Programs (Relay Protection System)

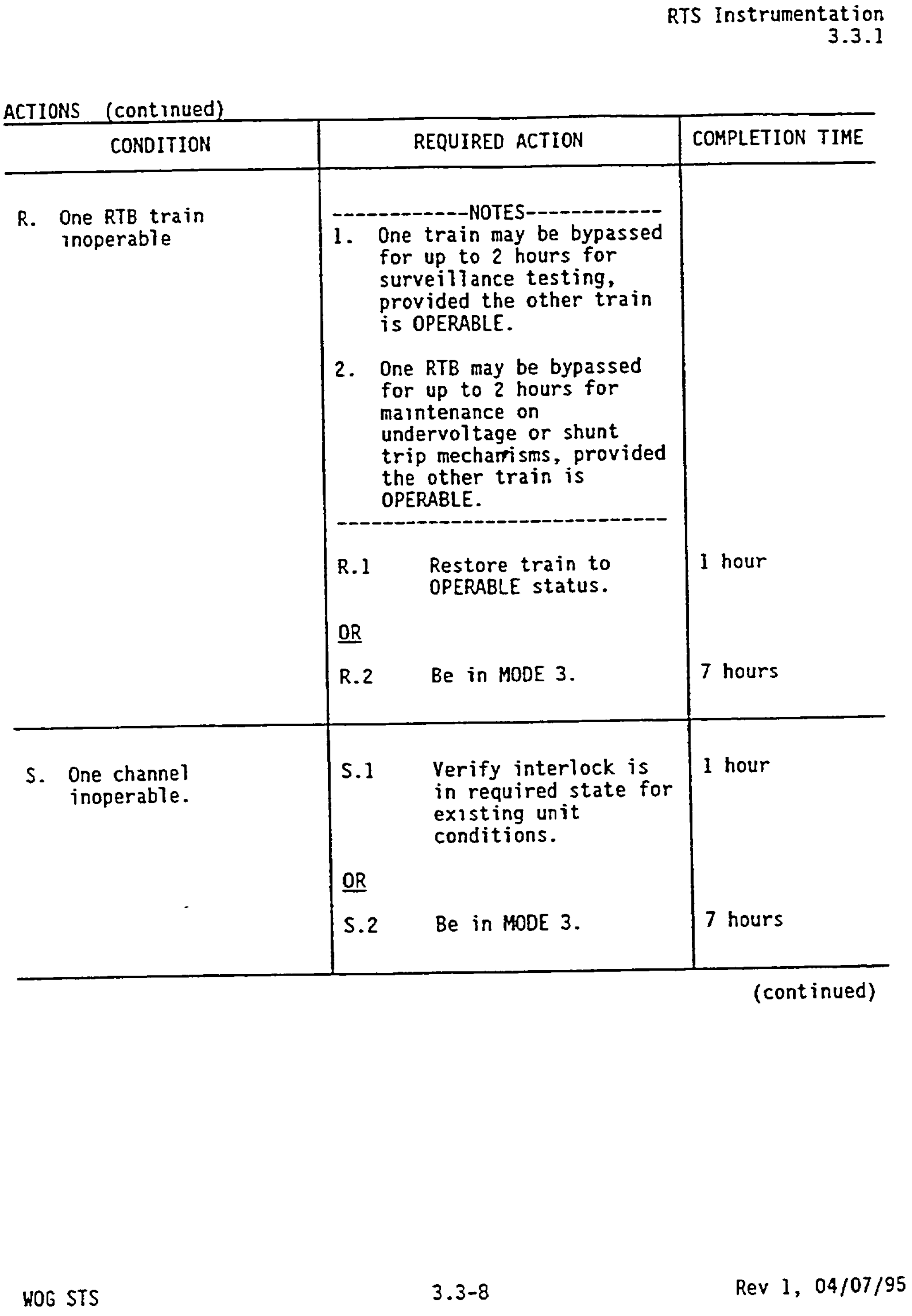
Component	Pre-TOP	WCAP-10271 (TOP)	WCAP-14333
Analog Channels			
- CT	1 hour	6 hours	72 hours
- Bypass Time	2 hours	4 hours	12 hours
- COT[2] STI	1 month	3 months	3 months
- Calibration Interval	NEAP[1]	NEAP[1]	18 months
- Calibration Tıme	NEAP[1]	NEAP[1]	4 hours
Logic Cabinet			
- CT	2 hours	6 hours	24 hours
- Bypass Tıme	3 hours	8 hours	8 hours
- STI	1 month	1 month	1 month
Master Relay			
- CT	6 hours	6 hours	24 hours
- Bypass Tıme	3 hours	8 hours	8 hours
- STI	1 month	1 month	1 month
Slave Relay			
- CT	6 hours	6 hours	24 hours
- Bypass Tıme	6 hours	12 hours	12 hours
- STI	3 months	3 months	3 months
Reactor Trip Breakers			
- CT	6 hours	6 hours	6 hours
- Bypass Time	2 hours	2 hours	2 hours
- STI	2 months	2 months	2 months

Notes

1) NEAP - Not Evaluated At-Power, previously this activity has typically been done while shutdown.

2) COT - Channel Operational Test (bypass or test tıme)

2.0 SPECIFIC RTS, ESFAS AND RELATED TECHNICAL SPECIFICATIONS EVALUATED



RTS Instrumentation
3.3.1

ACTIONS (continued)

CONDITION	REQUIRED ACTION	COMPLETION TIME
R. One RTB train inoperable	------------NOTES------------ 1. One train may be bypassed for up to 2 hours for surveillance testing, provided the other train is OPERABLE. 2. One RTB may be bypassed for up to 2 hours for maintenance on undervoltage or shunt trip mechanisms, provided the other train is OPERABLE. -----------------------------	
	R.1 Restore train to OPERABLE status.	1 hour
	OR	
	R.2 Be in MODE 3.	7 hours
S. One channel inoperable.	S.1 Verify interlock is in required state for existing unit conditions.	1 hour
	OR	
	S.2 Be in MODE 3.	7 hours

(continued)

WOG STS 3.3-8 Rev 1, 04/07/95

SURVEILLANCE REQUIREMENTS (continued)

	SURVEILLANCE	FREQUENCY
SR 3.3.1.4	--------------------NOTE-------------------- This Surveillance must be performed on the reactor trip bypass breaker prior to placing the bypass breaker in service. -- Perform TADOT.	31 days on a STAGGERED TEST BASIS
SR 3.3.1.5	Perform ACTUATION LOGIC TEST.	31 days on a STAGGERED TEST BASIS
SR 3.3.1.6	--------------------NOTE-------------------- Not required to be performed until [24] hours after THERMAL POWER is ≥ 50% RTP. -- Calibrate excore channels to agree with incore detector measurements.	[92] EFPD
SR 3.3.1.7	--------------------NOTE-------------------- Not required to be performed for source range instrumentation prior to entering MODE 3 from MODE 2 until 4 hours after entry into MODE 3. -- Perform COT.	[92] days

(continued)

SURVEILLANCE REQUIREMENTS

-----------------------------------NOTE-----------------------------------
Refer to Table 3.3.2-1 to determine which SRs apply for each ESFAS Function.

SURVEILLANCE		FREQUENCY
SR 3.3.2.1	Perform CHANNEL CHECK.	12 hours
SR 3.3.2.2	Perform ACTUATION LOGIC TEST.	31 days on a STAGGERED TEST BASIS
SR 3.3.2.3	-------------------NOTE------------------- The continuity check may be excluded. --- Perform ACTUATION LOGIC TEST.	31 days on a STAGGERED TEST BASIS
SR 3.3.2.4	Perform MASTER RELAY TEST.	31 days on a STAGGERED TEST BASIS
SR 3.3.2.5	Perform COT.	92 days
SR 3.3.2.6	Perform SLAVE RELAY TEST.	[92] days

(continued)

SURVEILLANCE REQUIREMENTS

-----------------------------------NOTE-----------------------------------
Refer to Table 3.3.6-1 to determine which SRs apply for each Containment Purge and Exhaust Isolation Function.

SURVEILLANCE		FREQUENCY
SR 3.3.6.1	Perform CHANNEL CHECK.	12 hours
SR 3.3.6.2	Perform ACTUATION LOGIC TEST.	31 days on a STAGGERED TEST BASIS
SR 3.3.6.3	Perform MASTER RELAY TEST.	31 days on a STAGGERED TEST BASIS
SR 3.3.6.4	Perform COT.	92 days
SR 3.3.6.5	Perform SLAVE RELAY TEST.	[92] days
SR 3.3.6.6	--------------------NOTE-------------------- Verification of setpoint is not required. --- Perform TADOT.	[18] months
SR 3.3.6.7	Perform CHANNEL CALIBRATION.	[18] months

SURVEILLANCE REQUIREMENTS (continued)

SURVEILLANCE		FREQUENCY
SR 3.3.7.3	Perform ACTUATION LOGIC TEST.	31 days on a STAGGERED TEST BASIS
SR 3.3.7.4	Perform MASTER RELAY TEST.	31 days on a STAGGERED TEST BASIS
SR 3.3.7.5	Perform SLAVE RELAY TEST.	[92] days
SR 3.3.7.6	--------------------NOTE----------------- Verification of setpoint is not required. --- Perform TADOT.	[18] months
SR 3.3.7.7	Perform CHANNEL CALIBRATION.	[18] months

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
B. (continued)	B.2.2.2 Perform SR 3.1.1.1.	1 hour AND Once per 12 hours thereafter

SURVEILLANCE REQUIREMENTS

SURVEILLANCE	FREQUENCY
SR 3.3.9.1 Perform COT.	[92] days
SR 3.3.9.2 Perform CHANNEL CALIBRATION.	[18] months

3.0 NEED FOR TECHNICAL SPECIFICATION STI AND CT CHANGES

The CT and STI changes for the RPS (RTS and ESFAS) components are necessary to reduce utility burden and reduce the probability of reactor trip during component testing activities. Testing of the analog channels, if not completed in bypass, places the reactor in a more vulnerable position with regard to a trip. Most plants do not have bypass test capability for the analog channels and need to test the channels in trip. To complete analog channel test activities, each analog channel is required to be actuated to the tripped state. During this activity, if another channel spuriously switches to the tripped state, then the reactor trip logic (2 of 3 or 2 of 4) is completed and a reactor trip, with possible actuation of safety systems will occur Testing of the other components of the RPS (logic cabinets, master relays, and RTBs) can also lead to plant trips or unnecessary actuations of safety systems.

For systems with low reliability, frequent testing may be necessary to verify that the system is operable, that is, has not failed due to passive component failures. However, for systems with relatively high reliability, testing requirements can be less frequent. The reactor protection system falls in the latter group; it is a highly reliable system. Previous studies of the reliability of the RPS, one of particular interest is the NRC's reliability study on the Westinghouse reactor protection system (Reference 7), verifies this statement. In addition, the RPS does not by itself provide generation of all reactor protection signals. The reactor operator provides a backup function to the RPS signal generation through the abilty to trip the reactor, initiate safety injection, and start all plant components from the control room when required to mitigate transient events that can adversely impact the reactor. The operators are trained and highly qualified to perform this function. Given that the RPS is a highly reliable system and is backed-up by operators, and that test activities can cause unnecessary reactor trips and component actuations, an extension to the RPS STIs that will have a negligible impact on plant safety and reduce the utility burden required to perform these activities is requested.

The CT and bypass time extensions are required to provide sufficient time to perform maintenance and test activities on the RTBs. This change is also requested to remove an inconsistency between the current CTs and bypass times between the RTBs and logic cabinets. Currently, the logic cabinets have a CT of 24 hours and a bypass time of 4 hours, however, the RTBs have a CT of 1 hour and a bypass time of 2 hours. This can result in the shorter RTB CT and bypass time limiting logic cabinet activities if tested concurrently. It is expected that an extension to the RTB CT or bypass time will have a negligible impact on plant risk due to the RPS testing and maintenance configuration. When the RTBs are in test or undergoing maintenance, its corresponding bypass breaker is placed in operation and actuated by the logic cabinet of the fully operable RPS train, that is, the reactor is still protected by two trip breakers. The extension in the CT and bypass time will also provide the reactor operators with flexibility when required to address issues related to the RPS reliability.

4.0 TECHNICAL SPECIFICATION CHANGE REQUEST

This analysis provides the justification for extending the surveillance test intervals for the analog channels, logic cabinets, master relays, and RTBs and the CTs and bypass times for the RTBs as indicated in Table 4.1 for the solid state protection system and Table 4.2 for the relay protection system.

Table 4.1 Summary of RPS STI and CT Changes - Solid State Protection System

Component	Surveillance Test Intervals	Completion Times and Bypass Times
Logic Cabinet	2 months to 6 months	No changes
Master Relays	2 months to 6 months	No changes
Analog Channels	3 months to 6 months	No changes
Reactor Trip Breakers	2 months to 4 months[1]	AOT: 1 hour to 24 hours Bypass Time: 2 hours to 4 hours

Notes

1) Initially evaluated an extension to 6 months, but the impact on CDF did not meet the acceptance guideline in Regulatory Guide 1 174.

Table 4.2 Summary of RPS STI and CT Changes - Relay Protection System

Component	Surveillance Test Intervals	Completion Times and Bypass Times
Logic Cabinet	1 month to 6 months	No changes
Master Relays	No change[2]	No changes
Analog Channels	3 months to 6 months	No changes
Reactor Trip Breakers	2 months to 4 months[1]	AOT: 1 hour to 24 hours Bypass Time: 2 hours to 4 hours

Notes

1) Initially evaluated an extension to 6 months, but the impact on CDF did not meet the acceptance guideline in Regulatory Guide 1.174

2) Due to component reliability, as discussed in Section 8 2 5, extensions to the STI for the master relays were not considered

5.0 NRC MEETING SUMMARY

At the start of the program, before the NRC issued their draft risk-informed Regulatory Guides and Standard Review Plans, the WOG met with the NRC to discuss the program. A summary of the key points of the meeting are provided below. At the start of this program, the WOG was considering STI extensions to 18 months. Several points in the following summary reflect this as noted at the end of the summary.

1. The NRC agreed that following a similar approach to that used for the previous programs evaluating changes to Technical Specification requirements for the RPS (References 3-6) is appropriate. That is, the use of representative signals to determine the impact on signal unavailability and the use of one representative plant specific PRA model to determine the impact on risk, as opposed to individual plant specific evaluations, is acceptable.

2. None of the changes to STIs for the logic cabinets, master relays, or RTBs, nor the change to the CT for the RTBs being proposed for evaluation are unacceptable to the NRC, that is, none of these changes are off limits. (Note that evaluation for increasing the analog channel STI to 6 months was added after the NRC meeting.)

3. A strong statement of need for the STI and CT extensions is necessary.

4. Use of the reactor trip and engineered safety feature actuation signal fault tree models from WCAP-10271 and WCAP-14333 analyses is acceptable.

5. Use of the risk analysis from the WCAP-14333 analysis is acceptable provided the NRC's current review of the model (as part of the in-progress review of WCAP-14333) finds it acceptable. (Note that an SER was subsequently issued for WCAP-14333.)

6. The analysis results should be referenced back to the pre-TOP and TOP (WCAP-10271) AOT and STI conditions.

7. Risk measures to be reported are the CDF, LERF, CCDF, and the increase in CCDP for AOT changes. Risk measures to be reported are the CDF and LERF for the STI changes.

8. The NRC would like to see a justification for applying the assumption for a linear relationship between component failure probability and test interval for the larger (18 month) intervals. The impact of the increased STI on common cause failure should also be addressed.

9. Sensitivity cases examining "how bad can it get" should be provided, that is, instead of using a mean component failure probability (the component failure rate x STI/2) use the component failure probability at the end of the test interval (the component failure rate x STI).

10. The NRC indicated that the WOG may wish to consider testing the components on a staggered basis to keep some type of check on potential common cause failures.

11. The NRC is concerned about not being able to detect the impact of loss of support (like cooling) on the component reliability for extensions up to 18 months under the proposed STI extensions as opposed to the current 2 months STI.

12. The NRC indicated that any available data regarding the reliability of these or similar components tested at longer STIs would be beneficial to the justification.

At the start of the program, STI increases to 18 months were being considered and discussed with the NRC. These STI extensions were reduced to the values provided in Section 4, as information related to the acceptance criteria in the risk-informed Regulatory Guides was issued and from the results of the finalized WCAP-14333 analyses. With this additional information and the generally conservative approach being taken in the analysis, and assuming that the component failure probability is linearly proportional to the STI, it was judged that 18 month STIs would be hard to justify. Based on this information, the STIs provided in Tables 4.1 and 4.2 were established.

Key points 8, 9, 10, and 11 were identified primarily due to the long STIs initially being considered. With reducing the STIs extensions to values significantly less than 18 months, these issues have not been addressed.

6.0 DESIGN BASIS REQUIREMENTS AND IMPACT

The following information is taken from the Bases of NUREG-1431, Rev. 1, for Westinghouse Plants.

The RPS consists of the reactor trip system (RTS) instrumentation and the engineered safety features actuation system (ESFAS) instrumentation. The RTS initiates a reactor shutdown based on values of selected parameters to protect against violating the core fuel design limits and reactor coolant system pressure boundary during anticipated operational occurrences, those events expected to occur one or more times during the unit life, and to assist the engineered safety features systems in mitigating accidents. The protection systems are designed to assure safe operation of the reactor. This is achieved by specifying limiting safety system settings, or trip setpoints, in terms of parameters directly monitored by the RTS, as well as specifying limiting conditions for operation (LCO) on other reactor system parameters and equipment performance. The RTS also protects against accidents, that is, events that are not expected to occur during the unit life. The acceptance limit during accidents is that offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 limits.

The ESFAS initiates necessary safety systems, based on the values of selected unit parameters, to protect against violating core design limits and the reactor coolant system pressure boundary, and to mitigate accidents.

The RTS instrumentation is divided into four parts: field transmitters or process sensors, signal process control and protection system, solid state or relay protection system, and reactor trip switchgear. Each part of the RTS instrumentation is designed with redundancy to meet design requirements. The field transmitter or sensors and signal process control and protection system typically consist of three or four channels and require two-out-of-four or two-out-of-three logic to meet the reliability requirements. The solid state or relay protection system and reactor trip switchgear consists of two trains with either one capable of tripping the reactor. A more detailed system description is provided in Section 7.0.

The ESFAS instrumentation is divided into three parts: field transmitters or sensors, signal processing equipment, and solid state or relay protection system. Each part of the ESFAS instrumentation is designed with redundancy to meet design requirements. The field transmitter or sensors and signal processing equipment typically consist of three or four channels and require two-out-of-four or two-out-of-three logic to meet the reliability requirements. The solid state or relay protection system consists of two trains with either one capable of actuating the required safety systems. The master relays and slave relays are included as part of the solid state and relay protection systems. A more detailed system description is provided in Section 7.0.

The RTS functions to maintain the safety limits during all anticipated operational occurrences and mitigates the consequences of design basis accidents in all modes in which the RTBs are closed. Each of the analyzed accidents and transients can be detected by one or more RTS functions. Plant accident analyses take credit for most RTS trip functions. RTS trip functions not specifically credited in the accident analysis are qualitatively credited in the safety analysis and the NRC staff approved licensing basis for the unit. These RTS trip functions may provide protection for conditions that do not require dynamic transient analysis to demonstrate function performance. They may also serve as backups to RTS trip functions that were credited in the accident analysis.

The LCO requires all instrumentation performing an RTS function to be operable. Failure of any instrument renders the affected channel(s) inoperable and reduces the reliability of the affected functions.

The LCO generally requires operability of four or three channels in each instrumentation function, two channels of manual reactor trip in each logic function, and two trains in each automatic trip logic function. Four operable instrumentation channels in a two-out-of-four configuration are required when one RTS channel is also used as a control system input. This configuration accounts for the possibility of the shared channel failing in such a manner that it creates a transient that requires RTS action. In this case, the RTS will still provide protection, even with random failure of one of the other three protection channels. Three operable instrument channels in a two-out-of-three configuration are generally required when there is no potential for control system and protection system interaction that could simultaneously create a need for RTS trip and disable one RTS channel. The two-out-of-three and two-out-of-four configurations allow one channel to be tripped during maintenance or testing without causing a reactor trip.

Each of the analyzed accidents can be detected by one or more ESFAS function. One of the ESFAS functions is the primary actuation signal for that accident. An ESFAS function may be the primary actuation signal for more than one type of accident. An ESFAS function may also be a secondary or backup actuation signal for one or more other accidents. Functions such as manual initiation, not specifically credited in the accident safety analysis, are qualitatively credited in the accident safety analysis and the NRC approved licensing basis for the unit. These functions may provide protection for conditions that do not require dynamic transient analysis to demonstrate function performance. These functions may also serve as backups to functions that were credited in the accident analysis.

The LCO requires all instrumentation performing an ESFAS function to be operable. Failure of any instrumentation renders the affected channel(s) inoperable and reduces the reliability of the affected functions.

The LCO generally requires operability of four or three channels in each instrumentation function and for two channels in each logic and manual initiation function. The two-out-of-three and two-out-of-four configurations allow one channel to be tripped during maintenance or testing without causing an ESFAS initiation. Two logic or manual initiation channels are required to ensure no single random failure disables the ESFAS.

Impact of Proposed Changes

The proposed changes include extending the surveillance test intervals for the analog channels, logic cabinets, master relays and RTBs, and extending the CT and bypass time for the RTBs. None of these changes impact the design basis requirements. As required in the design basis, RTS and ESFAS instrumentation will be available to protect the reactor during anticipated operational occurrences and accidents. Backup and redundant signals will remain available. None of the proposed changes will impact acceptance limits that protect against violating the core fuel design and reactor coolant system pressure boundary nor will they impact acceptance limits that protect against offsite dose requirements. In addition, the limiting safety system settings and instrumentation response times are not impacted by the proposed changes.

7.0 REACTOR PROTECTION SYSTEM DESCRIPTION

This section discusses the RTS and ESFAS instrumentation system design and performance of test and maintenance activities on the instrumentation system components.

7.1 RTS AND ESFAS DESIGN

The typical RTS circuit consists of analog channels (field transmitters or process sensors and signal process control and protection system), combinational logic units (solid state or relay protection system), and RTB (reactor trip switchgear). The typical ESFAS circuit consists of analog channels (field transmitters or sensors and signal processing equipment), combinational logic (solid state or relay protection system), and actuation relays. The analog channels, part of the process instrumentation system, provide signals to each of two logic cabinets which in turn provide signals to their respective reactor trip breakers and the actuation relays. The actuation relays consist of master and slave relays, with the master relays being controlled by the logic cabinet and the slave relays being controlled by the master relays. The slave relays actuate the required equipment. Figure 7.1 shows a simplified diagram of the overall reactor protection system.

Any particular protective feature, such as safety injection on pressurizer pressure low, will have either two, three, or four separate analog channels with each providing input to the logic cabinets. Actuation of the RTBs or master and slave relays requires a combinational logic of one-out-of-two, two-out-of-three, or two-out-of-four, as appropriate.

A typical analog channel consists of a sensor, loop power supply, signal conditioning circuits, and a comparator which is the output device to the logic cabinet. The sensor measures physical parameters such as temperature, pressure, level, etc The measurement is converted to an electrical signal and transmitted to the protection racks for signal conditioning. The signal conditioning modules perform a number of functions including amplification, square root derivation, lead/lag compensation, integration, summation, and isolation. A signal comparator, usually a bistable device, compares the conditioned signal to a predetermined setpoint and turns the output off or on if the voltage exceeds the setpoint. Each bistable controls two relays; one for train A logic and the other for train B logic.

The combinational logic is performed in the logic cabinet. Each logic cabinet consists of three bays; the input bay which contains the input relays, the logic bay, and the output bay which contains the master and slave relays. Two types of logic bays are used; solid state logic or relay logic

The solid state cabinet, or solid state protection system (SSPS), receives inputs from the analog channels via the input relays. This is accomplished using relays in either an energized or de-energized state, as determined by the output of the comparator The relays operate grounding contacts in the SSPS circuitry. When a comparator senses a trip condition the corresponding input relay will energize as appropriate, applying a ground to a specific logic input. The logic inputs are applied to universal boards which are the basic circuits of the protection system These boards contain one-out-of-two, two-out-of-three, or two-out-of-four logic circuits. Grounding of the appropriate number of universal board inputs will cause a signal to be generated. Output signals from the universal boards are connected to other universal boards, undervoltage output boards, or safeguard output boards as described:

1. Connection to other universal boards enables additional logic combinations. For example, auxiliary feedwater may be started by low level in one steam generator as sensed by 2 of 3 channels. Each of the three steam generator channels for one steam generator would input to a 2 of 3 universal board. For a three-loop plant there would be three such circuits. The output of each of these universal boards would input to a 1 of 3 universal board to achieve the desired logic.

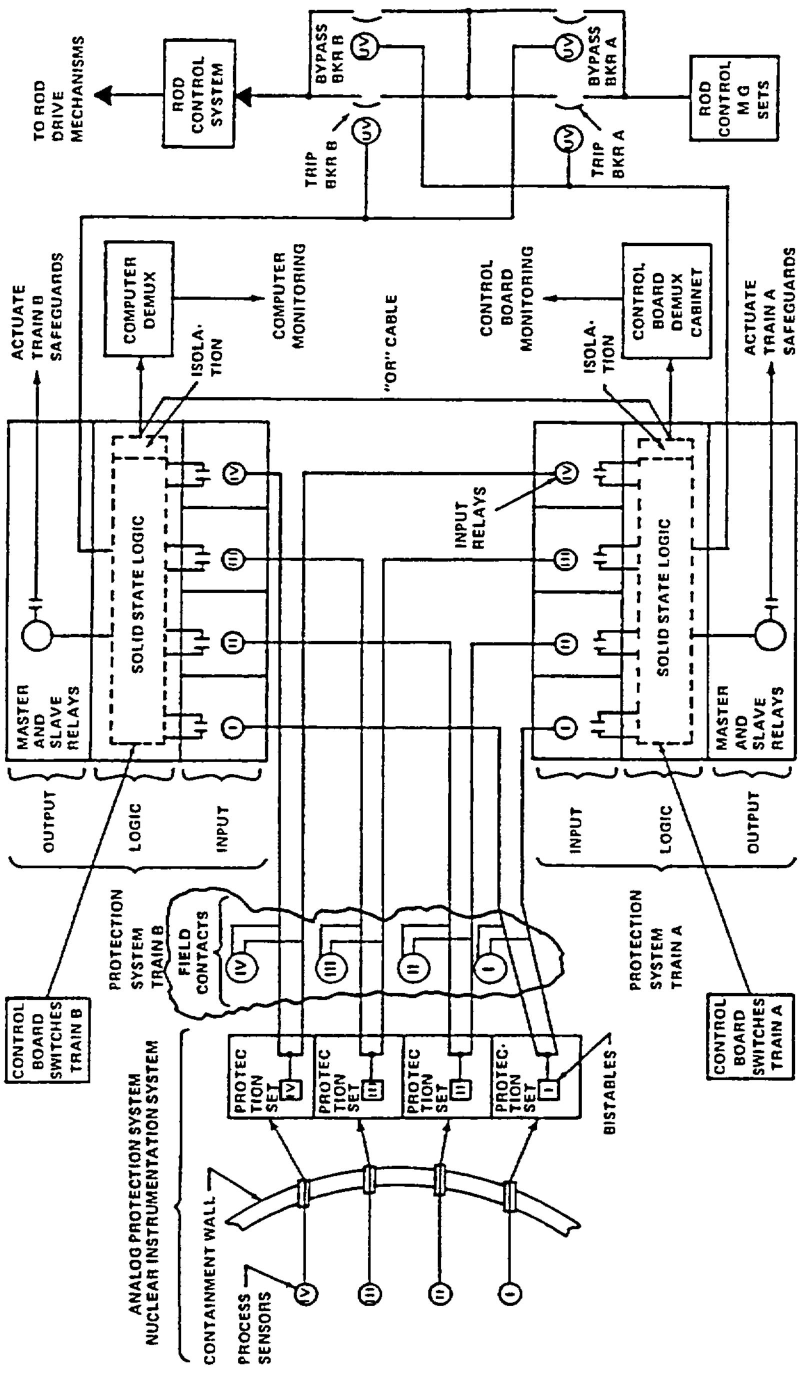
2. Connection to undervoltage output boards to drive the undervoltage relays to trip the RTBs.

3. Connection to safeguard output boards to drive the master relays which in turn drive the slave relays.

The relay logic (protection system) consists of contacts in a series-parallel arrangement which energize a master relay when appropriate combinations of contacts are closed, or de-energize a master relay when the appropriate combination of contacts are open, depending on the function. The series-parallel contacts are operated by the output relays of the analog channels and are arranged to initiate appropriate protective functions when the required number of analog channels sense an out-of-limit condition.

The master and slave actuation relays function to start the safeguards equipment which is used to mitigate events. This is accomplished by a combination of relay operations initiated by the output of the logic circuit. Each master relay energized by the logic circuit closes contacts which energize one or more slave relays. The number of master and slave relays is dependent on the particular protective function. The more complex the function, the greater the number of relays energized. Each slave relay when energized, closes contacts in the actuation circuits for one or more pieces of equipment. Typically each slave relay causes several components to operate.

Figure 7.1 Simplified Diagram of the Reactor Protection System



7.2 TEST AND MAINTENANCE ACTIVITIES

This program is concerned with test and maintenance activities related to the analog channels, logic cabinets, reactor trip breakers, and master relays in the RTS and ESFAS instrumentation systems. The protection system is designed to allow online testing. An overlapping test sequence is used, with each test within the testing scheme adequately testing a portion of the protection system. Satisfactory completion of all tests provides assurance that the system will perform as assumed in the safety analysis when demanded. Typically, testing of the protection system involves verification of the proper channel response to known inputs, proper comparator (bistable) settings and proper operation of the combinational logic and associated trip breakers, master relays, and slave relays. Details of RPS and ESFAS testing are provided in References 3 and 5.

With regard to the following analyses, the impact of test and maintenance activities on the RTS and ESFAS are important. Of specific interest is the impact on the availability of protection system signals. That is, how the individual components of the protective functions are degraded during test and maintenance activities.

Analog channels: The channels can be tested and maintained in either the bypassed or tripped state depending on the specific plant hardware capability. If tested in the bypassed state, the channel is unavailable and actuation logic changes from 2 of 3 to 2 of 2 or from 2 of 4 to 2 of 3 depending the initial logic requirement. If tested in the tripped state, the channel is providing a trip signal to the logic and then the additional logic required for actuation changes from 2 of 3 to 1 of 2 or from 2 of 4 to 1 of 3. Most plants do not have the installed bypass test capability, Eagle 21 process protection system, or the bypass test panel, therefore, the tripped state is typically used.

Logic cabinets: The logic is tested and maintained in the bypassed state. That is, the cabinet is unavailable during these activities.

Master relays: The master relays are tested and maintained in the bypassed state. That is, the relays are unavailable during these activities.

Slave relays: The slave relays are tested and maintained in the bypassed state. That is, the relays are unavailable during these activities.

Reactor trip breakers: The trip breakers are tested and maintained in the bypassed state, but the bypass trip breaker for the main trip breaker being tested or maintained is used to provided reactor trip function from two breakers. During such activities, the bypass breaker is controlled by the available (opposite train) logic.

With regard to maintenance activities, two types can be done; corrective and preventive. Corrective maintenance, or repair activities due to component failures, are those that are done after a component failure is identified through either a test or by some other means, such as through visual control room board scans. Preventive maintenance activities are pre-scheduled maintenance activities done to maintain the component in operable condition. Both types of activities impact the component availability.

8.0 ASSESSMENT OF IMPACT ON RISK

This section presents the analysis and assumptions used to determine the impact on plant risk of changing the Technical Specification requirements as shown in Tables 4.1 and 4.2. This section addresses the three-tiered approach to the evaluation of risk-informed Technical Specification changes. The first tier, discussed in Sections 8.1 to 8.4, addresses PSA insights and includes the RTS and ESFAS unavailability analyses, and risk analyses that support the risk impact assessment. The second tier discussed in Section 8.5, addresses avoidance of risk-significant plant configurations. The third tier discussed in Section 8.6, addresses risk-informed plant configuration control and management.

8.1 TIER 1: APPROACH TO THE EVALUATION

The Tier 1 analysis provides the impact of the changes on core damage frequency (CDF) and large early release frequency (LERF) for the STI changes and on CDF, incremental conditional core damage probability (ICCDP), LERF, and incremental conditional large early release probability (ICLERP) for the RTB CT and bypass time changes. The overall approach involved a three part process:

Part 1: Data analysis

The data analysis is used to determine failure rates or failure probabilities for the components that comprise the RPS. This information is used in the fault tree evaluation in Step 2 that determines the impact of the changes on signal unavailabilities. The data used is from several sources including the previous RTS and ESFAS studies (References 3-6), the NRC analysis of the Westinghouse RPS (Reference 7), and data collection from Westinghouse plants. This is discussed in detail in Section 8.2.

Part 2: RTS and ESFAS unavailability analysis

The unavailability analysis is required to determine the impact of the Tech Spec changes on the availability of the signals from the reactor protection system. Not all the RTS and ESFAS signals are modeled and evaluated with fault tree analysis. Consistent with the Reference 6 study, only representative signals are evaluated in detail. The representative signals used and the justification for their use are discussed in Section 8.1.1.

Part 3: Risk analysis

The risk analysis uses the results from the unavailability analysis to determine the impact of the changes on the appropriate risk parameters as noted above. A representative PRA model is used for this purpose. The use of this representative PRA is discussed in Section 8.1.2. An initial quantification of the PRA model using the CTs, bypass times, and STIs in WCAP-14333 that were approved by the NRC provides the base case which all the changes are compared against. Each change is evaluated individually and those that comprise the final group of changes to be requested are evaluated together.

8.1.1 Representative RPS Signals

The WOG WCAP-10271 analysis evaluated all the RTS and ESFAS signals specified in the Technical Specifications that are common to most plants. These are provided in Tables 3.2-2 and 3.2-3 of Reference 4 for reactor trip signals and in Tables 3.1-2 and 3.1-3 of Reference 5 for ESFAS signals.

Not all the fault trees developed and quantified in the WCAP-10271 effort were used in this current analysis; those evaluated were considered representative of the results for most of the other fault tree analyses. Only evaluating representative trees is adequate, since many of the fault tree analyses provided similar results in terms of signal unavailabilities and changes in signal unavailabilities. The following paragraphs provide the justification for the choice of representative signals. This is consistent with the approach used in the WCAP-14333 analysis.

One of the conclusions from the WOG TOP work was that the ESF actuation signals can be grouped, for signal unavailability type analyses, according to the number of master and slave relays, logic cabinet type (relay or solid state), and actuation logic (2 of 3 versus 2 of 4). This is concluded in Reference 5, and discussed in Section 6 of Reference 6, from the ESFAS unavailability results.

Reactor trip actuation signals can be grouped, for signal unavailability type analyses, according to logic type (relay or solid state) and actuation logic (2 of 3 versus 2 of 4), although for reactor trip actuation signals it is necessary to consider signals from diverse sets of actuating sources (diverse sets of analog channels) as well as from single sets of 2 of 3 and 2 of 4 logic. This can be seen from reviewing the signal unavailability results in Reference 3 and is also discussed in Section 6 of Reference 6.

Sections 6 1 and 6.2 of Reference 6 provide a detailed discussion of the signals identified as representative. This discussion is not repeated here. The following signals are identified as representative:

- Safety injection from pressurizer pressure low interlocked with P-11.
- Auxiliary feedwater pump start signal from steam generator level low-low in one loop.
- Reactor trip single source from pressurizer pressure high.
- Reactor trip diverse source from pressurizer pressure high or overtemperature delta T.

The safety injection signal and the reactor trip signals are evaluated with and without reactor trip. Table 8 1 provides a summary of the signals that were used in this evaluation.

Table 8.1 Summary of Signals Used in the Evaluation

Function	Logic Cabinet	Channel Logic	Operator Action
SI[1]	SSPS	2 of 3	No
SI[1]	SSPS	2 of 4	No
SI[1]	SSPS	2 of 3	Yes
SI[1]	SSPS	2 of 4	Yes
SI[1]	Relay	2 of 3	No
SI[1]	Relay	2 of 4	No
AFWPS[2]	SSPS	2 of 3	No
AFWPS[2]	SSPS	2 of 4	No
AFWPS[2]	Relay	2 of 3	No
AFWPS[2]	Relay	2 of 4	No
RT[3]	SSPS	2 of 3	No
RT[3]	SSPS	2 of 4	No
RT[4]	SSPS	Diverse	No
RT[3]	SSPS	2 of 3	Yes
RT[3]	SSPS	2 of 4	Yes
RT[4]	SSPS	Diverse	Yes
RT[3]	Relay	2 of 3	No
RT[3]	Relay	2 of 4	No
RT[4]	Relay	Diverse	No

Notes

1) SI signal is from pressurizer pressure low interlocked with P-11.

2) AFWPS signal is from steam generator level low-low in one loop

3) RT single source signal is from pressurizer pressure high.

4) RT diverse source signal is from pressurizer pressure high or overtemperature delta T.

8.1.2 Representative PRA Model

In selecting the plant PSA model to be used in the analysis several key factors were considered. These are:

- The engineered safety features actuation signals (ESFAS) must be incorporated into the model in sufficient detail to reflect the actuation signal/actuated system interface. Signals are required for actuation of engineered safety features such as emergency core cooling system, auxiliary feedwater pump start, main feedwater isolation, main steamline isolation, containment spray, and containment isolation.

- The PSA model must allow for crediting operator actions to actuate the safety systems if the automatic signals fail. The model must also be able to account for dependencies of subsequent operator actions on previous operator actions.

- The plant needs to have available procedures that direct the plant operators to initiate safety systems if automatic actuation fails.

- The PSA model must address anticipated transient without scram (ATWS) events (failure of the reactor trip signal).

- The plant needs to have available procedures that direct the operators to trip the plant and respond to an ATWS event if the automatic actuation fails.

- An inclusive set of initiating events along with detailed plant response (event) trees are required.

- Consistency in level of modeling detail between the actuation system and actuated systems and components is necessary.

- PRA model quality and completeness (with regard to the reactor protection system sıgnals to trip the reactor and initiate safety systems) ıs important.

The Vogtle Electric Generating Plant PRA model met all these requirements. It uses a support system approach and examined a full complement of internal events including internal flooding. The Vogtle PRA model includes a thorough examination of the signals required to actuate all the safety features, including reactor trip. ESFAS for safety injection are modeled in the support system event trees A nondiverse signal is modeled for all events requiring safety ınjectıon. Events also credit an operator action, as appropriate, to initiate safety injection via the SI switch in the control room. Appropriate actuation signals are included, as necessary, in the model for containment spray actuation, containment isolation, auxiliary feedwater pump start, main steam system ısolation, and emergency core cooling system recirculation.

Reactor trip actuation signals are included for all events as necessary. The small LOCA, steam generator tube rupture, and secondary side break events use a nondiverse signal for reactor trıp, and all the other events, except for large and medium type LOCAs, use a diverse sıgnal. The large and medium type

LOCA events do not require reactor trip; the reactor will shutdown due to voiding and injection of borated water. All events, except for large and medium type LOCAs, also credit manual reactor trip.

The level of detail for component modeling is consistent with regard to the components that the actuation signals are required to actuate. That is, the mechanical components that require actuation by the RPS are included in the Vogtle PRA model. This includes pumps that are required to start, valves that are required to change position, etc.

The Vogtle PRA model was developed in response to Generic Letter 88-20 (Individual Plant Examination). In many areas it exceeds the requirements to meet GL 88-20, such as the detail of modeling included for the reactor protection system (reactor trip and engineered safety features actuation signals). The model used in this analysis is the same as that developed to meet the Generic Letter with regard to the modeling of the reactor protection system and interaction of the protection system with other plant systems. It is also the same model that was used for the previous risk analysis (WCAP-14333). Therefore, the model is applicable for this evaluation

Applicability of Vogtle PRA to Other Plants

As noted above, of primary importance in selecting the plant PSA model to be used in the risk evaluation is the breadth of the modeling of the RPS, including the interface of the RPS with the actuated safety systems Of specific interest is how the reactor trip actuation signals and the engineered safety features actuation signals are incorporated into the model.

ESFAS signals are required for a number of safety features, such as, safety injection, auxiliary feedwater pump start, main feedwater isolation, etc. Detailed models for each of the actuation signals and the actuated systems are required. In addition, a detailed model of the reactor trip actuation signal(s) is required. As presented in this WCAP, the RPS including both the reactor trip and engineered safety features actuation signals, is similar across Westinghouse plants. There may be differences in the specific signals used to actuate a specific safety system or trip the reactor for a specific event, but the general design and function of the protection system is the same for all Westinghouse plants.

To properly evaluate the changes being considered in this analysis, the actuated systems and the interface between the actuation signals and actuated systems is the important factor. The number of loops in a plant is not critical. The exact design or configuration of each individual safety feature is not critical either; the function is the critical factor. All Westinghouse plants have the same basic safety functions and a similar set of actuating signals in addition to similar procedures that direct plant operators to manually initiate safety systems if the automatic signals fail, such as, manually starting the safety injection or manually starting auxiliary feedwater.

In general, all PRA models for Westinghouse plants consider a similar set of initiating events or accidents. The RPS functions similarly across all Westinghouse plants in response to this set of initiators. There are some plant specific events that need to be considered, but even many of these are similar across plants. Those that are plant unique typically are not significant contributors to plant risk and the RPS is not a significant contributor to plant risk from these events. The large contributors to risk are usually small and medium LOCAs, transient events, loss of offsite power/station blackout, loss of service water, and loss of component cooling water.

It should be remembered that the signal unavailability models developed and evaluated in this WCAP are used to replace the signal unavailability models in the Vogtle PRA model. Therefore, the signal unavailability models are not Vogtle specific, but are applicable to all Westinghouse plants.

Therefore, using one plant as representative of all Westinghouse plants is appropriate due to important high level similarities across plants that include:

- Safety functions (safety injection, auxiliary feedwater pump start, main steamline isolation, containment spray actuation, etc.)
- Reactor trip function
- RPS design and signal generation from similar parameters
- Common initiating events

It should also be noted that the ATWS event, caused by a reactor trip failure, has not been identified as an event that contributes significantly to plant risk. The actuated systems, not the actuation system, are usually the significant risk contributors.

8.1.3 General Quantification Process

The process to determine the impact of the STI, CT, and bypass time changes on plant risk as measured by core damage frequency and other risk parameters requires two separate quantifications. The first is the fault tree quantification which provides the signal unavailabilities and cutsets, and the second is the plant response (event) tree quantification which provides the CDF, LERF, and accident sequences. The following describes the process used in this analysis in more detail. It is assumed that the representative signals have already been identified and that the representative PRA model that will be used in the assessment has also been identified. As discussed in Section 8.1.2, the representative PRA model is the version of the Vogtle PRA model that was used in the previous analysis (WCAP-14333).

Step 1: Identify the actuation signals modeled in the representative plant PRA

A thorough review of the representative PRA model is necessary to identify where the reactor trip and engineered safety features actuation signals are incorporated into the model. Also identified are the signals modeled in the representative PRA for each protective function including credit for operator actions and diverse signals. This requires a detailed review of the support system model, plant response (event) trees, and system unavailability or fault tree analyses. The following actuation signals are included in the model:

Reactor trip

Safety injection

Auxiliary feedwater pump start

Containment spray

Main feedwater isolation

Steamline isolation

Step 2: Identify the signals to be used for the evaluation

The signals to be used in the risk analysis are identified, which requires a review of the initiating events that could occur, how a plant would respond to these events, and what is modeled in the representative PRA (see Step 1). Also considered is the availability of diverse signals and the opportunity for the operators to manually actuate safety systems if the automatic signals fail. Tables 8.1 and 8.2 of WCAP-14333 provide a summary of this information. Based on this information, the following signals are evaluated via fault tree analysis to determine actuation signal unavailabilities:

- Reactor trip on pressurizer pressure high (nondiverse) with operator action
- Reactor trip on pressurizer pressure high or overtemperature delta T (diverse) with operator action
- Safety injection on pressurizer pressure low interlocked with P-11
- Safety injection on pressurizer pressure low interlocked with P-11 with operator action
- Auxiliary feedwater pump start on steam generator level low-low in one loop (also used as the general or representative signal with regard to unavailability for main feedwater isolation and steamline isolation)

Step 3: Calculate the actuation signal unavailabilities

Signal unavailabilities are calculated for the reactor trip and engineered safety features actuation signals listed in Step 2. The fault trees that model these signals are discussed in Section 8.3. The fault trees are evaluated for each individual change being considered and a combined case of all the changes to be requested. As noted above, the base case represents the changes approved in WCAP-14333. The Westinghouse WesSAGE code system (Reference 9) is used for the fault tree quantification.

The common cause failure contribution is added into the signal unavailability in a step separate from the fault tree quantification. To do this, the cutsets from the fault tree quantification are reviewed for common cause contributors and then the appropriate calculations are done to determine the common cause contribution. Common cause contributions for the slave relays, master relays, reactor trip breakers, logic cabinets, analog channels. and power supplies are included. The approach for common cause failure is discussed in Section 8.3

Step 4: Factor signal unavailability values into the representative plant PRA model

The actuation signal unavailabilities calculated in Step 3 are factored into the appropriate places in the PRA model. This step requires that the values be entered in the appropriate data files that are used in the PRA model CDF quantification. Any additional calculations that need to be done with respect to these values, such as crediting manual actuation of individual components for safety injection, are completed at this point.

The reactor trip signal unavailability values are entered directly in the master data file. Two sets of safety injection signals are entered; one directly and the other after additional calculations. The additional calculations account for the operator action to manually re-align and start the required ECCS components for safety injection if the automatic signal fails.

The general signal unavailability values (auxiliary feedwater pump start) are included with the system they are required to actuate. The unavailability analyses for these systems (auxiliary feedwater, containment spray, and steam generator isolation) need to be re-evaluated with the new signal unavailabilities. These new system unavailabilities are then also entered into the master data file used in the CDF quantification.

Step 5: PRA Model Quantification

The PRA model plant response (event) trees are re-quantified at this point with all the modified data ın place. The Westinghouse QT code system (Reference 10) is used for this purpose. This quantification provides the core damage frequency, accident sequences, and the plant damage state frequencies for each case. Each new quantification requires that the appropriate data files be modified to reflect the parameter changes. This involves changing the parameters previously discussed.

8.2 DATA DEVELOPMENT

8.2.1 Introduction

The component failure probability data was obtained from several sources. A key change in this analysis, as discussed in Section 8 3.3, is modeling the components in the logic cabinents at the card level instead of the component level and combining the various failure modes for the master relays and relay logic cabinet input relays into a single component failure basic event. These changes were made since the component specific reliability information based nuclear industry experience is available at these levels. Previously, generic data was used at the component level instead of the card level for logic cabinet compoents and for specific relay failure modes.

Updated failure probability data was used only for the components that were being evaluated for revised STIs. Those components that were not impacted by the STI changes used the same failure probability information that was used in the previous studies. For several components, failure probabilities were developed as part of this program and are discussed in Section 8.2.2 to 8.2.5. The following summarizes the component failure probabilities that were used. These values are based on the current STIs:

• Undervoltage driver card	3.37E-04/d (Reference 7)
• Universal logic card	3.83E -04/d (Reference 7)
• Output relay	3.94E-05/d (Reference 7)
• Bistable/comparator	7.46E-04/d (Reference 7)
• Pressure sensor	1.16E-04/d (Reference 7)
• Pressure signal processing	1.57E-04/d (Reference 7)
• Temperature sensor	5.98E-04/d (Reference 7)
• Reactor trip breaker	3.70E-05/d (based on Reference 7)
• Level sensor	1.16E-04/d (assumed to be similar to pressure sensor)
• Level signal processing	1.57E-04/d (assumed to be similar to pressure signal processing)
• Slave relays	same as previous studies (References 3-6)
• 118 VAC power supply	same as previous studies (References 3-6)
• 48 VDC power supply	same as previous studies (References 3-6)
• 15 VDC power supply	same as previous studies (References 3-6)
• Loop power supply	same as previous studies (References 3-6)
• Master relays (SSPS)	developed in this program (see Sections 8.2.2 to 8.2 5)
• Safeguard driver card (SSPS)	developed in this program (see Sections 8.2.2 to 8.2.5)
• Master relays (Relay Protection System)	developed in this program (see Sections 8.2.2 to 8.2.5)

RPS and ESFAS components are located in cabinets where the environment (temperature, humidity, vibration, debris, dust, etc.) is more controlled than similar components used in industrial applications. In a controlled environment, electrical components are expected to be more reliable than components subjected to hostile environments.

8.2.2 Components Included in Survey

Failure probabilities were determined for the selected RPS and ESFAS components listed in Section 8 2.1. The new failure probabilities were determined by using plant operating experience rather than the generic industry reliability factors in WCAP-10271 and its Supplements. Plant operating experience for the selected components are documented in utility surveys. The plants that participated in the survey and the results of the surveys are provided in Tables 8.2 through 8.5 ın Section 8.2.3. The assumptions used for calculating the new reliabılity factors are listed in Section 8.2.4. New reliability factors for the components listed in Section 8.2.2 are provided in Section 8.2 5.

Based upon utility surveys, failure probabilities were calculated for the following selected components:

- SSPS Master Relays

Relay Type	Model Number
CP Clare	GP1R21D3000
P&B	KHU17D12-48
Midtex	156-14D200
Midland Ross	156-14C300

- SSPS Safeguards Dnver Cards
- Relay Protection System Input Logic Relays (Westinghouse BF and BFD input logic relays in relay protection system designs)
- Relay Protectıon System Master Relays (Westinghouse MG-6 master relays in relay protection system designs)

8.2.3 Plant Survey

A survey was sent to utilities in order to obtain component operating experience data for selected electrical components. Component reliabılity was determined from the responses to this survey. A copy of the survey (Reference 11) ıs provıded in Appendix A.

Tables 8 2 through 8 5 provide a summary of the results of the surveys. Column 1 of each table identifies the plants that partıcıpated in the survey. Column 2 of each table is the number of

Table 8.2 SSPS Master Relays

a,c

Plant	Number of Surveillances	Unsafe Failures[1]

Note:

1) Unsafe failures are failures that preclude satisfying the safety function

Table 8.3 SSPS Safeguards Driver Cards

a,c

Plant	Number of Surveillances	Unsafe Failures[1]

Note.

1) Unsafe Failures are failures that preclude satisfying the safety function.

Table 8.4 Relay Protection System Input Logic Relays

a.c

Plant	Number of Surveillances	Unsafe Failures[1]

Note.

1) Unsafe Failures are failures that preclude satisfying the safety function.

Table 8.5 Relay Protection System Master Relays

a,c

Plant	Number of Surveillances	Unsafe Failures[1]

Note.

1) Unsafe Failures are failures that preclude satisfying the safety function

surveillance tests (demands) performed at each plant. Column 3 of each table is the number of unsafe failures. Unsafe failures are defined as failures that preclude satisfying the safety function.

8.2.4 Calculation Methodology

Determination of failure probabilities is primarily dependent on two factors, the number of demands and the number of failures to operate on demand. The total number of demands was determined by multiplying the number of components installed in the plant by the plant specific technical specification (NUREG 1431, Rev. 1) test frequency, times the number of test intervals (starting from the commercial operation date through the completion of the survey). The number of failures was determined from the survey responses Where survey responses were not specific enough to determine if the failures were unsafe (i.e., the failure would prevent the component from completing its safety function), other sources such as, Licensee Event Reports (LER) and follow-up phone surveys were used to clarify data provided in the surveys. Failure probabilities were determined by dividing the total number of failures to actuate on demand by the total number of demands.

The following assumptions were used for calculatıng the reliability factors in Tables 8.2 through 8.5 in Section 8 2.3:

- Plants with Solid State Protection Systems test safeguards driver cards on one train each month
- Plants with Solid State Protection Systems test master relays on one train each month
- Plants with Relay Protection Systems test input logic relays on one train each month and on all functions each quarter
- Plants with Relay Protection Systems test master relays either on one train each month or once each refueling outage depending on the installed test capability
- Refueling outage interval assumed is 18 months for all plants

8.2.5 Summary

Based upon the results of utility input to the WOG survey (Reference 11), new failure probabilities (failures/demand) were calculated and are listed in Table 8.6. Based on the results presented in Table 8.6, it is apparent that the failure probability of the relay protection system master relays is much higher than the reliabilıty of the SSPS master relays. Due to this high failure probability it was judged that increasing the STI for these relays was not an appropriate action. The failure probabilities of the other components in this table are consistent with other similar components, and they remain candidates for STI extensions.

Table 8.6 Component Failure Probabilities

a,c

Table	Component	Failures/Demand

8.3 RTS AND ESFAS SIGNAL UNAVAILABILITY ANALYSIS

As discussed in Section 8.1, the approach used in this analysis is consistent with that used in previous WOG programs evaluating changes to RTS STIs and CTs. A fault tree analysis was used to assess the impact of the CT and bypass time changes on the unavailability of reactor trip and engineered safety features actuation signals. These unavailabilities were then used in a risk analysis to determine the impact on plant safety.

This section of the report presents and discusses the signal unavailability analysis. It includes a discussion on the approach, assumptions, fault tree models, and the results.

8.3.1 Unavailability Analysis Approach

The approach used in this analysis to determine the impact of the changes on signal unavailability is based on fault trees. The fault trees used are based on those previously used in WCAP-14333. These fault trees model the unavailability of the signal given a particular signal demand. Several changes were made to the details of the fault trees and these are discussed in the subsequent sections. Each fault tree specifically models and is unique to a particular RPS and ESFAS signal. Fault trees were developed for each signal noted in Table 8.1. The fault tree models are discussed in Section 8.3.3.

The assumptions (see Section 8.3.2) are consistent with the previous studies (References 3-6). Signal unavailabilities were calculated for the cases shown in Tables 8.7 and 8.8 for the SSPS and Relay Protection System, respectively. Changes to the STIs and CTs for a specific parameter are reflected in each case. The Base Case is taken from WCAP-14333. The final case provides an evaluation of the complete set of STI and CT changes.

The analysis included contributions to signal unavailabilities from the following sources:

- Random failures of components
- Common cause failures of components
- Unavailability of components due to testing
- Unavailability of components due to maintenance
- Human error

Included in the fault tree models are the hardware failures, operator actions, and test and maintenance activities which can lead to signal failure These are discussed in detail in Section 4.1 of Reference 3.

For the most part, the fault trees do not specifically include component common cause failure contributions to signal unavailability. This is added by hand calculations after quantification of the fault trees. The Multiple Greek Letter (MGL) and Beta Factor common cause approaches are used in this analysis. This is consistent with the common cause approach used for the reactor trip breakers, master and slave relays, logic cabinets and analog channels in WCAP-14333.

The common cause failure approach and the approach to assess the unavailability of components due to maintenance and test activities are discussed further in the following paragraphs.

Common Cause Failures

The MGL method was used to determine common cause failure contributions to signal unavailability for the analog channels. The Beta Factor approach was used for the RTB, logic cabinet components, master relays and slave relays.

In applying the Beta Factor approach to multiple failures of the reactor trip breakers, master relays, slave relays, and logic cabinets, the following Beta factors were used:

Reactor trip breakers – 0.043

Master relays – [ ]^{a,c}

Slave relays – [ ]^{a,c}

Power supplies – [ ]^{a,c}

Universal logic card – 0.044

Undervoltage driver card – 0.029

Safeguards driver card – [ ]^{a,c}

Test, blocking and RT contacts – [ ]^{a,c}

(These values are based on References 5, 6, and 7.)

In applying the MGL approach to the analog channels, the following equations are used:

Failure of 3 of 4 components: Q x β x γ x (1-δ)/3 x no. of common cause cutsets

Failure of 4 of 4 components: Q x β x γ x δ x no. of common cause cutsets

Failure of 2 of 3 components: Q x β x (1-γ)/2 x no. of common cause cutsets

Failure of 3 of 3 components: Q x β x γ x no. of common cause cutsets

where: Q - component failure probability

β - Beta factor = [ ]^{a,c}

γ - Gamma factor = [ ]^{a,c}

δ- Delta factor = [ ]^{a,c}

The Beta factors for the slave relays, master relays, power supplies, and test, blocking, and RT contacts along with the Beta, Gamma, and Delta factors for the analog channel components are from Reference 6. The Beta factors for the reactor trip breakers, universal logic cards, and undervoltage driver cards are based on information provided in Reference 7. The Beta factor for the safeguards driver cards is assumed to be similar to the Beta factors for the other similar components; in this case the universal logic cards and the undervoltage driver cards.

In determining the common cause contribution of the analog channels, it is necessary to determine the detection interval for component failures. Failure of some of the components that comprise the channels will be detected within a shift, while others will only be detected during the Channel Operational Test (COT) (quarterly for TOP implementation and the 184 days for this assessment). Component failures that can be detected during a shift are those that can be observed by control board scans. These include sensor and loop power supply failures. Component failures that are only detectable by the COT are for comparators, output relays, and signal conditioning circuitry.

Component Unavailability Due to Test and Maintenance Activities

The following calculations demonstrate the component test and maintenance unavailability approach. The failure data presented is for the Base Case scenario.

Logic cabinet test unavailability for the reactor trip breaker

= (4 hrs/test)/(2 months/test x 730 hrs/month)

= 2.74E-03

where: test interval is 2 months

test time is 4 hours

Analog channel test and calibration unavailability

= (12 hrs/test)/(3 months/test x 730 hrs/month)) +

((4 hrs/calibration)/(18 months/calibration x 730 hrs/month))

= 5.78E-03

where: test interval is 3 months and test time is 12 hours

calibration interval is 18 months and calibration time is 4 hours

Master relay and logic cabinet test unavailability for AFW

= ((4 hrs/test)/(2 months/test x 730 hrs/month)) +

((4 hrs/test)/(2 months/test x 730 hrs/month))

= 5 48E-03

where: master relay test interval is 2 months and test time is 4 hours

logic cabinet test interval is 2 months and test time is 4 hours

Reactor trip breaker test unavailability

= (2 hrs/test)/(2 months/ test x 730 hrs/month)

= 1.37E-03

where: reactor trip breaker test interval is 2 months reactor trip breaker test time is 2 hours

Reactor trip breaker maintenance unavailability

= (6 hrs/(1 yr x 8760 hrs/yr))

= 6.85E-04

where: reactor trip breaker maintenance interval is one year

reactor trip breaker maintenance time is 6 hours

Component Failure Probabilities

The component failure probabilities were calculated in one of two ways dependent on the available data. For components with a known failure rate, the failure probability was calculated by:

FP = FR x STI/2

where: FP - failure probability

FR - failure rate

For components with a known failure probability based on a particular STI, the component failure probability for an extended test interval was determined by increasing the current failure probability by a factor equal to the test interval increase as shown by:

FP (extended STI) = FP (current STI) x (extended STI/current STI)

This assumes a linear relation between failure probability and the STI which is consistent with the failure rate approach shown above.

Table 8.7 Solid State Protection System Cases

Parameter	Base Case	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6[1]	Combined Case
Analog Channels								
- Maint. Time	72+6 hours	72+6 hours	72+6 hours	72+6 hours	72+6 hours	72+6 hours	72+6 hours	72+6 hours
- Maint Interval	2 years	2 years	2 years	2 years	2 years	2 years	2 years	2 years
- Test (bypass) time	12 hours	12 hours	12 hours	12 hours	12 hours	12 hours	12 hours	12 hours
- Test Interval	3 months	***6 months***	3 months	3 months	3 months	3 months	3 months	***6 months***
- Calibration Interval	18 months	18 months	18 months	18 months	18 months	18 months	18 months	18 months
- Calibration Time	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours
Logic Cabinet								
- Maint. Time	24+6 hours	24+6 hours	24+6 hours	24+6 hours	24+6 hours	24+6 hours	24+6 hours	24+6 hours
- Maint Interval	18 months	18 months	18 months	18 months	18 months	18 months	18 months	18 months
- Test (bypass) Time	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours
- Test Interval	2 months	2 months	***6 months***	2 months	2 months	2 months	2 months	***6 months***
Master Relays								
- Maint Time	24+6 hours	24+6 hours	24+6 hours	24+6 hours	24+6 hours	24+6 hours	24+6 hours	24+6 hours
- Maint. Interval	see Note 1	See Note 1	see Note 1	see Note 1	see Note 1	see Note 1	see Note 1	see Note 1
- Test (bypass) Time	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours
- Test Interval	2 months	2 months	2 months	***6 months***	2 months	2 months	2 months	***6 months***

Note 1: Maintenance interval is based on the component failure rate

Table 8.7 Solid State Protection System Cases (cont.)

Parameter	Base Case	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Combined Case
Slave Relays								
- Maint. Time	24+6 hours	24+6 hours	24+6 hours	24+6 hours	24+6 hours	24+6 hours	24+6 hours	24+6 hours
- Maint. Interval	see Note 1	See Note 1	see Note 1	see Note 1	see Note 1	see Note 1	see Note 1	see Note 1
- Test (bypass) Time	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours
- Test Interval	3 months	3 months	3 months	3 months	3 months	3 months	3 months	3 months
Reactor Trip Breakers								
- Maint. Time	6 hours	6 hours	6 hours	6 hours	6 hours	***24+6 hours***	6 hours	***24+6 hours***
- Maint. Interval	1 year	1 year	1 year	1 year	1 year	1 year	1 year	1 year
- Test Time	2 hours	2 hours	2 hours	2 hours	2 hours	***4 hours***	2 hours	***4 hours***
- Test Interval	2 months	2 months	2 months	2 months	***6 months***	2 months	***4 months***	***4 months***

Note 1: Maintenance interval is based on the component failure rate

Table 8.8 Relay Protection System Cases

Parameter	Base Case	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
Analog Channels							
- Maint. Time	72+6 hours	72+6 hours	72+6 hours	N/A	72+6 hours	72+6 hours	72+6 hours
- Maint. Interval	2 years	2 years	2 years	N/A	2 years	2 years	2 years
- Test (bypass) time	12 hours	12 hours	12 hours	N/A	12 hours	12 hours	12 hours
- Test Interval	3 months	***6 months***	3 months	N/A	3 months	3 months	3 months
- Calibration Interval	18 months	18 months	18 months	N/A	18 months	18 months	18 months
- Calibration Time	4 hours	4 hours	4 hours	N/A	4 hours	4 hours	4 hours
Logic Cabinet							
- Maint. Time	24+6 hours	24+6 hours	24+6 hours	N/A	24+6 hours	24+6 hours	24+6 hours
- Maint Interval	12 months	12 months	12 months	N/A	12 months	12 months	12 months
- Test (bypass) Time	4 hours	8 hours	8 hours	N/A	8 hours	8 hours	8 hours
- Test Interval	1 month	1 month	***6 months***	N/A	1 month	1 month	1 month
Master Relays							
- Maint Time	24+6 hours	24+6 hours	24+6 hours	N/A	24+6 hours	24+6 hours	24+6 hours
- Maint. Interval	see Note 1	see Note 1	see Note 1	N/A	see Note 1	see Note 1	see Note 1
- Test (bypass) Time	8 hours	8 hours	8 hours	N/A	8 hours	8 hours	8 hours
- Test Interval	1 month	1 month	1 month	N/A	1 month	1 month	1 month

Note 1: Maintenance interval is based on the component failure rate

Table 8.8 Relay Protection System Cases (cont.)

Parameter	Base Case	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
Slave Relays							
- Maint. Time	24+6 hours	24+6 hours	24+6 hours	N/A	24+6 hours	24+6 hours	24+6 hours
- Maint. Interval	see Note 1	see Note 1	see Note 1	N/A	see Note 1	see Note 1	see Note 1
- Test (bypass) Time	12 hours	12 hours	12 hours	N/A	12 hours	12 hours	12 hours
- Test Interval	3 months	3 months	3 months	N/A	3 months	3 months	3 months
Reactor Trip Breakers							
- Maint Time	6 hours	6 hours	6 hours	N/A	6 hours	***24+6 hours***	6 hours
- Maint. Interval	1 year	1 year	1 year	N/A	1 year	1 year	1 year
- Test Time	2 hours	2 hours	2 hours	N/A	2 hours	***4 hours***	2 hours
- Test Interval	2 months	2 months	2 months	N/A	***6 months***	2 months	***4 months***

Note 1: Maintenance interval is based on the component failure rate

8.3.2 Assumptions

The following presents the key assumptions for developing the fault tree models with regard to test and maintenance activities. Most of these are presented in References 3 and 5, but are repeated here for convenience.

8.3.2.1 Analog Channels

These assumptions are applicable to the analog channels as they are used in both the relay protection systems and solid state protection systems.

1. Analog channel testing and calibration activities are performed in the bypassed state. All plants do not routinely test in bypass; but for those that do, this is representative, and for those that do not, this is conservative.

2. Maintenance of the analog channels is performed in the bypassed state. This represents actual plant practice. Only corrective maintenance is performed at-power.

8.3.2.2 Solid State Protection System

The followmg assumptions are applicable to the logic cabinets, reactor trip breakers, master relays, and slave relays in a SSPS.

1. Testing of the logic prohibits automatic actuation of the entire associated train. This is consistent with hardware design and is necessary to allow at-power testing The redundant train remains operable and capable of providing all protective features

2. Maintenance of the logic cabinets is assumed to prohıbit actuatıon of the entire associated train. This is consistent with actual practice and conservative.

3. Testing of the reactor tnp breakers prohıbits actuation of the breaker in test. The bypass breaker corresponding to the affected breaker is placed into service and will be actuated by the logic cabinet in the unaffected train. This is consistent with actual practice.

4. Maintenance of the reactor trip breakers prohıbits actuation of the breaker in maintenance. The bypass breaker corresponding to the affected breaker is placed into service and will be actuated by the logic cabinet in the unaffected traın. This is consistent with actual practice.

5. Testing of the master relays prohibits actuation of the entire associated train. This is consistent with the test circuitry provided for the master relays and represents actual practıce.

6 Maintenance of the master relays makes the affected master relay and all associated slave relays inoperable. This is consistent with the design of the actuation relays.

7. The ESFAS signal is assumed to be unavailable if the equivalent relays, either master or slaves, in the redundant trains are unavailable. That is, if the relays that actuate the high head safety

injection pumps in each train are unavailable, the ESF function is assumed to be unavailable. This is conservative, since partial system failures are equated to total system failures. A less conservative approach, while appropriate, would require a significant increase in the complexity of the fault trees.

8. Testing and maintenance of slave relays was modeled assuming that only the affected relay is inoperable. This is consistent with actual practice and conservative. In many cases, the test actuates the associated components; therefore, the components remain available. However, in some cases, actuation of the components is blocked rendering the components unavailable for automatic actuation. Since the latter test scheme represents the limiting case, it was used for the model.

9. The number of master and slave relays actuated by an ESFAS signal varies from signal to signal and is a function of the number of components required to be actuated. Based on a review of several SSPS plant specific designs, the following is included in the models:

   - Safety Injection, and Containment Spray and Phase B Isolation: two master relays each driving three slave relays

   - Steamline Isolation, Main Feedwater Isolation, and Auxiliary Feedwater Pump Start: one master relay driving two slave relays

8.3.2.3 Relay Protection System

The hardware design varies for the relay protection system as discussed in Reference 5. A bounding configuration was identified by a review of several designs. The following assumptions are applicable to the logic cabinets, reactor trip breakers, master relays, and slave relays in a relay protection system.

1. Items 1 to 7 in Section 8.3.2.2 for the SSPS are applicable to relay protection systems also.

2. Maintenance of the slave relays was modeled assuming that the affected relay is inoperable. This is consistent with the SSPS modeling. Testing of the slave relay was modeled as to prohibit actuation of the entire associated train. This is consistent with actual practice and conservative.

3. The number of master and slave relays actuated by an ESFAS signal varies from signal to signal and is a function of the number of components required to be actuated. The following is included in the models:

   - Safety Injection: one master relay driving six slave relays

   - Steamline Isolation, and Containment Spray and Phase B Isolation: one master relay driving three slave relays

   - Auxiliary Feedwater Pump Start and Feedwater Isolation: one master relay directly driving the required components (no slave relays)

8.3.3 Fault Tree Models

Signal specific fault trees were used for each signal evaluated. These are listed in Table 8.1. Both single and dual train fault trees are modeled for the ESFAS. Dual train and diverse train fault trees are modeled for the RPS. The fault trees in this analysis are based on those in WCAP-14333. In WCAP-14333, however, each fault tree model of the system under consideration consists of multiple fault trees. For example, the safety injection dual train 2/4 logic with operator action model consists of an upper (models dual train master and slave relays plus a portion of the logic cabinets), middle (models the rest of the logic cabinets) and a lower (models the analog channels) tree. By combining many of the components, as explained in the following paragraphs, the upper middle and lower trees respective to that system can now be combined into one tree.

In this analysis, the multiple master relay failure modes have been combined into one failure event. In previous studies, the logic cabinets were modeled to the component level. In this study, the modeling is done at the card level.

These changes were done because industry-specific failure probability data is now available at the card level and because industry-specific data for the master relays was collected and analyzed. In previous analyses, the failure probability data was generic, since nuclear industry specific reliability data was not available for these components. This generic data was not necessarily representative of the operation of these components in the nuclear industry. Now with card level failure data available, improved models can be developed that more accurately model signal actuation availability.

The fault trees were quantified with the WesSAGE Computer Code (Reference 9). WesSAGE is a software tool used to develop and quantify fault trees. The output of the code provides the mean probability of failure and cutsets for the requested gate(s). The mean probability of failure and common cause contributions are discussed in the following section. All the fault trees used in this analysis are included in Appendix D.

8.3.4 Results of the Signal Unavailability Analysis

The signal unavailabilities for the representative safety injection and auxiliary feedwater pump start functions are provided on Tables 8.9 and 8.10, respectively, for the solid state protection system. Table 8.11 provides the signal unavailabilities for the representative safety injection and auxiliary feedwater pump start functions for the relay protection system. The signal unavailabilities for the representative reactor trip functions are provided in Tables 8.12 and 8.13 for the solid state and relay protection systems, respectively. In these tables, unavailability values, with and without common cause contributions, are given for the proposed cases for failure of the signal given both trains are supported, and given only a single train is supported. As previously mentioned, the CTs, bypass times or test times, surveillance test intervals, and maintenance intervals that correspond to these three cases (SI, AFW and RT) are provided on Tables 8.7 and 8.8 for the SSPS and relay protection system, respectively The following representative signals were used in the unavailability evaluation·

Solid State Protection System·

1. Safety injection on pressurizer pressure low interlocked with P-11: representative of the safety injection, and the containment spray and phase B isolation signals.

2. Auxiliary feedwater pump start on steam generator level low-low in one loop: representative of the auxiliary feedwater pump start, steamline isolation, and main feedwater isolation signals

3. Reactor trip on pressurizer pressure high; representative of all single source reactor trip signals.

4 Reactor trip on pressurizer pressure high or overtemperature delta T: representative of all diverse source signals.

Relay Protection System·

1. Safety injection signal: representative of the safety injection signal.

2. Auxiliary feedwater pump start signal: representative of the auxiliary feedwater pump start signal and the main feedwater isolation signal.

3. The signal unavailability results for steamline isolation, containment spray and containment isolation signals fall between the results for the safety injection and auxiliary feedwater pump start signals, so they were not specifically evaluated. It is conservatively assumed that the representative safety injection signal represents these signals also.

4. Reactor trip on pressurizer pressure high: representative of all single source reactor trip signals.

5. Reactor trip on pressurizer pressure high or overtemperature delta T: representative of all diverse source signals.

From Tables 8.9 through 8.13, the followıng general conclusions are reached. Several of these conclusions were previously provided in Reference 5.

1. The unavailabilities of engineered safety features actuation signals and the reactor trip actuation signals with 2 of 4 logic are lower than those corresponding signals with 2 of 3 logıc.

2. The unavailabilıties of engineered safety features and the reactor trip actuation signals with credit for an alternate actuation by operator action are lower than those corresponding signals without the operator action

3. Common cause failure contributions account for a considerable part of the total signal unavailability.

4. The ESFAS single train signal unavailabilities for the Proposed Case are lower than the signal unavailabilities for the Base Case. This is directly related to the trade-off between the increased component failure probability and the decreased component unavailability due to the increased test interval.

5 The signal unavailabilities and changes in signal unavailabilities between the three cases for the relay protection system are comparable to or less than the corresponding solid state protection system signals

6. The unavailabilities for the auxiliary feedwater pump start signal are lower than the unavailabilities for the safety injection signal (without operator action). As seen in the discussion below, this is primarily due to the number of master and slave relays modeled in each of these signals.

Tables 8.14 through 8.20 provide a breakdown of the signal unavailability by contributors. The contributors, or components, listed separately are the 1) random failures, test, and maintenance of the relays (masters and slaves), logic cabinets and analog channels, 2) common cause failures of the master relays, 3) common cause failures of the slave relays, 4) common cause failures of the logic cabinets, and 5) common cause failures of the analog channels. This information is pnmarily provided only for signals generated by the SSPS with 2 of 4 logic. In addition to the signal unavailability, the percent contribution for each contributor to the total signal unavailability is provided.

From this information, it is concluded that the contribution, or importance, of the analog channels and logic cabinets is significantly reduced when an operator action to actuate the protective feature is included in the model. The reason for this is that the operator action provides an alternate path, separate from the analog channels and logic cabinets, to actuate the master and slave relays or the reactor trip breakers. This is evident by comparing the results provided on Table 8.14 with those on Table 8.15 for safety injection signals and by comparing the results provided on Table 8.17 with those on Table 8.18 for the reactor trip feature. It is also concluded from this information that when diversity of signals to generate a reactor trip is considered, again the contribution, or importance, of the analog channels and logic cabinets is significantly reduced. This is related to the additional analog channels or logic trains that need to fail for the signal to fail. This is evident from a comparison of the results provided on Table 8.17 with those on Table 8.19. It is further concluded that when diversity of signals to generate a reactor trip is considered along with an operator action to generate the same trip, the components of primary importance are the reactor trip breakers. In this case, multiple analog channels or logic trains need to fail in addition to the operator action, and since the operator action, for the most part, is a backup to the logic cabinets and analog channels, these components are reduced to small contributors to signal unavailability. This can be seen by reviewing the results provided on Table 8.20 and comparing them with the results on Tables 8.17, 8.18 and 8 19.

It is also concluded from these tables, that the primary difference between the unavailability of the safety injection signal and the auxiliary feedwater pump start signal is related to the number of master and slave relays required for success of the protective feature. As shown in the fault tree models, the safety injection function includes two master relays per train, with each master actuating three slave relays, and the auxiliary feedwater pump start signal includes one master relay per train actuating two slave relays. Due to the additional master and slave relays required for the safety injection signal, there are more component failure combinations that will lead to failure of the signal. This can be seen from a comparison between the contributor breakdown provided on Table 8.14 for the safety injection signal and the breakdown provided on Table 8.16 for the auxiliary feedwater pump start signal. In particular, this is illustrated by a comparison of the common cause contributions for the master and slave relays.

Similar conclusions would apply if the detailed signal unavailability contributors were provided for signals generated from 2 of 3 logic or from relay protection systems. These conclusions are independent of the type of logic cabinet and analog channel logic.

The conclusions regarding diversity of signals and operator action backup to initiate the protective function are important when assessing the impact of the changes in the signal unavailability on plant safety. It is important to realize that all of the reactor trip signals are backed up by either a diverse signal or an operator action, and in many cases by both. This is also true for engineered safety features actuation signals. Many of these signals, dependent on the specific event being considered, can be generated by diverse sources or by operator actions.

The cutsets leading to failure of the signal for a sample of safety injection, auxiliary feedwater pump start, and reactor trip signals are provided in Tables 8.21, 8.22 and 8.23. Table 8.24 provides a key to the basic event identifiers used in these tables. These identifiers correspond to those in the fault trees in Appendix B. The cutsets provided for the safety injection signal are for pressurizer pressure low with 2/4 logic interlocked with P-11. The cutsets provided for the auxiliary feedwater pump start signal are for steam generator level low-low in one loop with 2/4 logic. The cutsets provided for the reactor trip signal are for pressurizer pressure high with 2/4 logic. These cutsets along with common cause contributions represent more than 90% of the total signal unavailability in each case. It is seen from these tables, that failure of the master relays, slave relays, logic cabinets, and analog channels by common cause are the major contributors to signal unavailability.

Based on the results of the unavailability analysis, it is concluded that the Technical Specification changes being considered in this assessment have a minor impact on the availability of the reactor trip and engineered safety features actuation signals. This is particularly evident for functions that are backed by either diverse actuation signals or operator actions. It is further concluded that the impact of the changes on signal unavailability for the SSPS can be used to represent the impact of the changes on signals generated by the relay protection system. This is based on a review and comparison of the signal unavailability results for the relay protection system with the results for the SSPS. Such a comparison indicates that the impact of the changes on the unavailability values from the Base Case (WCAP - 14333) to the Proposed Case (Combined AOTs and STIs) are comparable for both types of protection systems. In addition, the signal unavailability values for the relay protection system are consistently smaller that those for the SSPS Based on this, it is concluded that the SSPS results are representative of the relay protection system results.

Table 8.9 Summary of Safety Injection Unavailabilities: Solid State Protection System

Signal	Base Case	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Combined Case
SI - 2/4 logic w/ CCF	8.96E-04	9.26E-04	1.39E-03	8.61E-03	8.96E-04	8.96E-04	8.96E-04	1.34E-03
SI - 2/4 logic, w/o CCF	2.18E-04	2.18E-04	4.80E-04	1.76E-04	2.18E-04	2.18E-04	2.18E-04	4.01E-04
SI - 2/4 logic w/OA, w/ CCF	6.05E-04	6.05E-04	5.97E-04	5.87E-04	6.05E-04	6.05E-04	6.05E-04	5.79E-04
SI - 2/4 logic w/OA, w/o CCF	8.52E-05	8.52E-05	7.45E-05	6.09E-05	8.52E-05	8.52E-05	8.52E-05	4.98E-05
SI - 2/4 logic, 1 train, w/ CCF	2.74E-02	2.74E-02	3.05E-02	2.39E-02	2.74E-02	2.74E-02	2.74E-02	2.70E-02
SI - 2/4 logic, 1 train w/o CCF	2.74E-02	2.74E-02	3.05E-02	2.38E-02	2.74E-02	2.74E-02	2.74E-02	2.69E-02
SI - 2/4 logic, 1 train w/OA, w/ CCF	2.49E-02	2.49E-02	2.32E-02	2.14E-02	2.49E-02	2.49E-02	2.49E-02	1.96E-02
SI - 2/4 logic, 1 train w/OA, w/o CCF	2.49E-02	2.49E-02	2.32E-02	2.14E-02	2.49E-02	2.49E-02	2.49E-02	1.96E-02
SI - 2/3 logic, w/ CCF	1.12E-03	1.24E-03	1.61E-03	1.08E-03	1.12E-03	1.12E-03	1.12E-03	1.66E-03
SI - 2/3 logic, w/o CCF	3.56E-04	3.79E-04	6.19E-04	3.14E-04	3.56E-04	3.56E-04	3.56E-04	5.62E-04
SI - 2/3 logic w/OA, w/ CCF	6.07E-04	6.08E-04	5.99E-04	5.89E-04	6.07E-04	6.07E-04	6.07E-04	5.82E-04
SI - 2/3 logic w/OA, w/o CCF	8.62E-05	8.62E-05	7.65E-05	6.19E-05	8.62E-05	8.62E-05	8.62E-05	5.14E-05
SI - 2/3 logic, 1 train, w/ CCF	2.76E-02	2.77E-02	3.07E-02	2.41E-02	2.76E-02	2.76E-02	2.76E-02	2.73E-02
SI - 2/3 logic, 1 train, w/o CCF	2.75E-02	2.75E-02	3.06E-02	2.40E-02	2.75E-02	2.75E-02	2.75E-02	2.71E-02
SI - 2/3 logic, 1 train w/OA, w/ CCF	2.49E-02	2.49E-02	2.32E-02	2.14E-02	2.49E-02	2.49E-02	2.49E-02	1.96E-02
SI - 2/3 logic, 1 train w/OA, w/o CCF	2.49E-02	2.49E-02	2.32E-02	2.14E-02	2.49E-02	2.49E-02	2.49E-02	1.96E-02

Table 8.10 Summary of Auxiliary Feedwater Pump Start Signal Unavailabilities: Solid State Protection System

Signal	Base Case	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Combined Case
AFWPS - 2/4 logic, w/ CCF	3.41E-04	3.65E-04	5.32E-04	3.35E-04	3.41E-04	3.41E-04	3.41E-04	5.40E-04
AFWPS - 2/4 logic, w/o CCF	6.30E-05	6.30E-05	1.27E-04	5.38E-05	6.30E-05	6.30E-05	6.30E-05	1.09E-04
AFWPS - 2/4 logic, 1 train, w/ CCF	1.41E-02	1.41E-02	1.49E-02	1.23E-02	1.41E-02	1.41E-02	1.41E-02	1.32E-02
AFWPS - 2/4 logic, 1 train, w/o CCF	1.40E-02	1.40E-02	1.49E-02	1.22E-02	1.40E-02	1.40E-02	1.40E-02	1.31E-02
AFWPS - 2/3 logic, w/CCF	5.40E-04	6.38E-04	7.30E-04	5.34E-04	5.40E-04	5.40E-04	5.40E-04	8.13E-04
AFWPS - 2/3 logic, w/o CCF	1.90E-04	2.05E-04	2.54E-04	1.81E-04	1.90E-04	1.90E-04	1.90E-04	2.51E-04
AFWPS - 2/3 logic, 1 train, w/CCF	1.43E-02	1.44E-02	1.51E-02	1.25E-02	1.43E-02	1.43E-02	1.43E-02	1.34E-02
AFWPS - 2/3 logic, 1 train, w/o CCF	1.42E-02	1.42E-02	1.50E-02	1.24E-02	1.42E-02	1.42E-02	1.42E-02	1.33E-02

SI. Safety Injection
AFWPS. Auxiliary Feedwater Pump Start
CCF: Common Cause Failures
OA: Operator Action

Table 8.11 Summary of Safety Injection and Auxiliary Feedwater Pump Start Signal Unavailabilities: Relay Protection System

Signal	Base Case	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
SI - 2/4 logic, w/CCF	1.02E-03	1.04E-03	1.05E-03	N/A	1.02E-03	1.02E-03	1.02E-03
SI - 2/4 logic, w/o CCF	2.84E-04	2.85E-04	2.19E-04	N/A	2.84E-04	2.84E-04	2.84E-04
SI - 2/3 logic, w/CCF	1.24E-03	1.36E-03	1.28E-03	N/A	1.24E-03	1.24E-03	1.24E-03
SI - 2/3 logic, w/o CCF	4.24E-04	4.46E-04	3.59E-04	N/A	4.24E-04	4.24E-04	4.24E-04
AFWPS - 2/4 logic, w/CCF	2.36E-04	2.61E-04	3.46E-04	N/A	2.36E-04	2.36E-04	2.36E-04
AFWPS - 2/4 logic, w/o CCF	5.00E-05	5.00E-05	7.70E-05	N/A	5.00E-05	5.00E-05	5.00E-05
AFWPS - 2/3 logic, w/CCF	4.35E-04	5.33E-04	5.01E-04	N/A	4.35E-04	4.35E-04	4.35E-04
AFWPS - 2/3 logic, w/o CCF	1.76E-04	1.91E-04	1.62E-04	N/A	1.76E-04	1.76E-04	1.76E-04

SI. Safety Injection
AFWPS. Auxiliary Feedwater Pump Start
CCF: Common Cause Failures

Table 8.12 Summary of Reactor Trip Signal Unavailabilities: Solid State Protection System

Signal	Base Case	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6	Combined Case
RT - 2/4 logic, w/CCF	7.92E-05	1.08E-04	1.52E-04	7.92E-05	8.18E-05	8.53E-05	8.01E-05	1.95E-04
RT - 2/4 logic, w/o CCF	1.38E-05	1.41E-05	3.34E-05	1.38E-05	1.33E-05	1.99E-05	1.32E-05	4.61E-05
RT - 2/4 logic w/OA, w/CCF	2.74E-06	3.03E-06	3.33E-06	2.74E-06	6.65E-06	2.80E-06	4.68E-06	5.56E-06
RT - 2/4 logic w/OA, w/o CCF	5.00E-07	5.00E-07	5.63E-07	5.00E-07	1.24E-06	5.64E-07	8.65E-07	9.26E-07
RT - 2/3 logic, w/CCF	3.01E-04	4.24E-04	3.74E-04	3.01E-04	3.04E-04	3.07E-04	3.02E-04	5.11E-04
RT - 2/3 logic, w/o CCF	1.52E-04	1.75E-04	1.72E-04	1.52E-04	1.52E-04	1.58E-04	1.52E-04	2.07E-04
RT - 2/3 logic w/OA, w/CCF	4.96E-06	6.19E-06	5.56E-06	4.96E-06	8.87E-06	5.03E-06	6.91E-06	8.73E-06
RT - 2/3 logic w/OA, w/o CCF	1.89E-06	2.12E-06	1.95E-06	1.89E-06	2.63E-06	1.95E-06	2.25E-06	2.54E-06
RT - diverse signals, w/CCF	2.69E-05	2.71E-05	6.50E-05	2.69E-05	3.02E-05	2.99E-05	2.84E-05	7.28E-05
RT - diverse signals, w/o CCF	6.58E-06	6.58E-06	1.46E-05	6.58E-06	6.71E-06	9.62E-06	6.47E-06	2.06E-05
RT - diverse signals w/OA, w/CCF	2.22E-06	2.22E-06	2.47E-06	2.22E-06	6.14E-06	2.25E-06	4.17E-06	4.35E-06
RT - diverse signals w/OA, w/o CCF	4.34E-07	4.34E-07	3.80E-07	4.34E-07	1.18E-06	4.66E-07	8.04E-07	6.80E-07

RT: Reactor Trip
CCF: Common Cause Failures
OA: Operator Action

Table 8.13 Summary of Reactor Trip Signal Unavailabilities: Relay Protection System

Signal	Base Case	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
RT - 2/4 logic, w/CCF	6.09E-05	9.00E-05	1.74E-04	N/A	6.45E-05	6.14E-05	6.50E-05
RT - 2/4 logic, w/o CCF	3.81E-06	4.17E-06	7.46E-06	N/A	5.82E-06	4.33E-06	4.78E-06
RT - 2/3 logic, w/CCF	2.83E-04	4.06E-04	3.97E-04	N/A	2.87E-04	2.84E-04	2.87E-04
RT - 2/3 logic, w/o CCF	1.43E-04	1.66E-04	1.47E-04	N/A	1.45E-04	1.43E-04	1.44E-04
RT - diverse signals, w/CCF	1.13E-05	1.15E-05	4.68E-05	N/A	1.49E-05	1.18E-05	1.55E-05
RT - diverse signals, w/o CCF	3.27E-06	3.27E-06	6.92E-06	N/A	5.28E-06	3.79E-06	4.24E-06

RT Reactor Trip
CCF Common Cause Failures

Table 8.14 Breakdown of Signal Unavailability Contributors - SSPS Safety Injection: Pressurizer Pressure Low (2/4) Interlocked with P-11

	Unavailability Contributions			
	Base Case		**Combined STIs and AOTs Case**	
Contributor	**Unavailability**	**Percent**	**Unavailability**	**Percent**
Random failures, test & maint.	2.18E-04	24.3	4 01E-04	29.9
Common cause failures				
- Master relays	3.30E-06	0.4	9.90E-06	7.4
- Slave relays	5.15E-04	57.5	5.15E-04	38 4
- Safeguards driver card	2.95E-05	3.3	8.85E-05	6.6
- Universal logic card	8 45E-05	9.4	2.53E-04	18.9
- Power Supply: 118V AC	5.40E-06	0.6	5 40E-06	0 4
- Power Supply: 48V DC	3 60E-06	0.4	3 60E-06	0 3
- Power supply: 15VDC	3 60E-06	0.4	3 60E-06	0 3
- Analog channels	3 35E-05	3.7	6.23E-05	4 7
- Subtotal	6 78E-04	75.7	9 41E-04	70.2
Total	8 96E-04	See Note 1	1.34E-03	See Note 1

Note.

1) The total may not equal 100% due to round off.

Table 8.15 Breakdown of Signal Unavailability Contributors - SSPS Safety Injection: Pressurizer Pressure Low (2/4) Interlocked with P-11 with Operator Action

	Unavailability Contributions			
	Base Case		Combined STIs and AOTs Case	
Contributor	Unavailability	Percent	Unavailability	Percent
Random failures, test & maint.	8 52E-05	14.1	4 98E-05	8.6
Common cause failures				
- Master relays	3 30E-06	0 5	9 90E-06	1.7
- Slave relays	5 15E-04	85.1	5 15E-04	89.0
- Safeguards driver card	2.95E-07	0 05	8.85E-07	0.2
- Universal logic card	8 45E-07	0.1	2.53E-06	0.4
- Power Supply: 118V AC	5.40E-08	0.009	5.40E-08	0.009
- Power Supply: 48V DC	3.60E-08	0.006	3.60E-08	0.006
- Power supply: 15VDC	3.60E-08	0.006	3.60E-08	0.006
- Analog channels	3.35E-07	0.06	6.23E-07	0.1
- Subtotal	5.20E-04	86 0	5.29E-04	91.4
Total	6 05E-04	See Note 1	5 79E-04	See Note 1

Note:

1) The total may not equal 100% due to round off

Table 8.16 Breakdown of Signal Unavailability Contributors - SSPS Auxiliary Feedwater Pump Start: Steam Generator Level Low-Low in One Loop (2/4)

	Unavailability Contributions			
	Base Case		Combined STIs and AOTs Case	
Contributor	Unavailability	Percent	Unavailability	Percent
Random failures, test & maint.	6.30E-05	18.5	1.09E-04	20.2
Common cause failures				
- Master relays	1.65E-06	0.5	4.95E-06	0.9
- Slave relays	1.72E-04	50.4	1.72E-04	31.8
- Safeguards driver card	2.95E-05	8.7	8.85E-05	16.4
- Universal logic card	3.38E-05	9.9	1.01E-04	18.7
- Power Supply: 118V AC	5.40E-06	1.6	5.40E-06	1.0
- Power Supply: 48V DC	3.60E-06	1.1	3.60E-06	0.7
- Power supply: 15VDC	3.60E-06	1.1	3.60E-06	0.7
- Analog channels	2.87E-05	8.4	5.27E-05	9.7
- Subtotal	2.78E-04	81.5	4.32E-04	79.9
Total	3.41E-04	See Note 1	5 40E-04	See Note 1

Note

1) The total may not equal 100% due to round off

Table 8.17 Breakdown of Signal Unavailability Contributors - SSPS Reactor Trip: Pressurizer Pressure High (2/4)

	Unavailability Contributions			
	Base Case		Combined STIs and AOTs Case	
Contributor	Unavailability	Percent	Unavailability	Percent
Random failures, test & maint.	1.38E-05	17.4	4.61E-05	23.6
Common cause failures				
- Reactor trip breakers	1.60E-06	2.0	3.18E-06	1.6
- Undervoltage driver card	9.77E-06	12.3	2.93E-05	15.0
- Universal logic card	1.69E-05	21.3	5.06E-05	26.0
- Power supply: 15VDC	3.60E-06	4.6	3.60E-06	1.8
- Analog channels	3.35E-05	42.3	6.23E-05	32.0
- Subtotal	6.54E-05	82.6	1.49E-04	76.4
Total	7.92E-05	See Note 1	1.95E-04	See Note 1

Note:

1) The total may not equal 100% due to round off.

Table 8.18 Breakdown of Signal Unavailability Contributors - SSPS Reactor Trip: Pressurizer Pressure High (2/4) with Operator Action

	Unavailability Contributions			
	Base Case		Combined STIs and AOTs Case	
Contributor	Unavailability	Percent	Unavailability	Percent
Random failures, test & maint.	5.00E-07	18.2	9.26E-07	16.7
Common cause failures				
- Reactor trip breakers	1.60E-06	58.4	3.18E-06	57.2
- Undervoltage driver card	9.77E-08	3.6	2.93E-07	5.3
- Universal logic card	1.69E-07	6.2	5.06E-07	9.1
- Power supply: 15VDC	3.60E-08	1.3	3.60E-08	6.5
- Analog channels	3.35E-07	12.2	6.23E-07	11.2
- Subtotal	2.24E-06	81.6	4.64E-06	83.5
Total	2.74E-06	See Note 1	5.56E-06	See Note 1

Note.

1) The total may not equal 100% due to round off.

Table 8.19 Breakdown of Signal Unavailability Contributors - SSPS Reactor Trip: Pressurizer Pressure High (2/3) or Overtemperature Delta T (2/4)

	Unavailability Contributions			
	Base Case		Combined STIs and AOTs Case	
Contributor	Unavailability	Percent	Unavailability	Percent
Random failures, test & maint.	6.58E-06	24.5	2.06E-05	28.3
Common cause failures				
- Reactor trip breakers	1.60E-06	6.0	3.18E-06	4.4
- Undervoltage driver card	9.77E-06	36.3	2.93E-05	40.2
- Universal logic card	5.26E-06	19.6	1.58E-05	21.7
- Power supply: 15VDC	3.60E-06	13.4	3.60E-06	4.9
- Analog channels	8.50E-08	0.3	3.10E-07	0.4
- Subtotal	2.03E-05	75.5	5.22E-05	71.7
Total	2.69E-05	See Note 1	7.28E-05	See Note 1

Note:

1) The total may not equal 100% due to round off.

Table 8.20 Breakdown of Signal Unavailability Contributors - SSPS Reactor Trip: Pressurizer Pressure High (2/3) or Overtemperature Delta T (2/4) with Operator Action

Contributor	Unavailability Contributions			
	Base Case		Combined STIs and AOTs Case	
	Unavailability	Percent	Unavailability	Percent
Random failures, test & maint.	4.34E-07	19.6	6.80E-07	15.6
Common cause failures				
- Reactor trip breakers	1.60E-06	72.1	3.18E-06	73.1
- Undervoltage driver card	9.77E-08	4.4	2.93E-07	6.7
- Universal logic card	5.26E-08	2.4	1.58E-07	3.6
- Power supply: 15VDC	3.60E-08	1.6	3.60E-08	0.8
- Analog channels	8.50E-10	0.04	3.10E-09	0.07
- Subtotal	1.79E-06	80.6	3.67E-06	84.4
Total	2.22E-06	See Note 1	4.35E-06	See Note 1

Note:

1) The total may not equal 100% due to round off.

Table 8.21 Dominant Cutsets for Signal Failure - Combined Case SSPS Safety Injection: Pressurizer Pressure Low (2/4) Interlocked with P-11

CCF	5.15E-04	Slave relays		
CCF	2.53E-04	Universal logic cards		
CCF	8.85E-05	Safeguards driver cards		
CCF	6.23E-05	Analog channels		
CCF	9.90E-06	Master relays		
CCF	5.40E-06	118V AC power supply		
CCF	3.60E-06	48V DC power supply		
CCF	3.60E-06	15V DC power supply		
1.	4.84E-06	-TATSI	TBTSI	SGDCF
2.	4.84E-06	TATSI	-TBTSI	SGDEF
3.	3.23E-06	SRD3T	SRF3T	SGDCF
4.	3.23E-06	SRD3T	-SRF3T	SGDEF
5.	3.23E-06	-SRD2T	SRF2T	SGDCF
6.	3.23E-06	SRD2T	-SRF2T	SGDEF
7.	3.23E-06	-SRD1T	SRF1T	SGDCF
8.	3.23E-06	SRD1T	-SRF1T	SGDEF
9.	3.23E-06	-SRC3T	SRE3T	SGDCF
10.	3.23E-06	SRC3T	-SRE3T	SGDEF
11.	3.23E-06	-SRC2T	SRE2T	SGDCF
12.	3.23E-06	SRC2T	-SRE2T	SGDEF
13.	3.23E-06	-SRC1T	SRE1T	SGDCF
14.	3.23E-06	SRC1T	-SRE1T	SGDEF
15.	3.14E-06	-TATSI	TBTSI	UL313CF
16.	3.14E-06	-TATSI	TBTSI	UL416CF
17.	3.14E-06	-TATSI	TBTSI	UL308CF
18.	3.14E-06	-TATSI	TBTSI	UL315CF
19.	3.14E-06	-TATSI	TBTSI	UL404CF
20.	3.14E-06	TATSI	-TBTSI	UL313EF
21.	3.14E-06	TATSI	-TBTSI	UL416EF
22.	3.14E-06	TATSI	-TBTSI	UL308EF
23.	3.14E-06	TATSI	-TBTSI	UL315EF
24.	3.14E-06	TATSI	-TBTSI	UL404EF
25.	3.13E-06	SGDCF	SGDEF	

See Table 8 24 for descripuons of basic event idenufiers.

Table 8.22 Dominant Cutsets for Signal Failure – Combined Case SSPS Auxiliary FW Pump Start: Steam Generator Level Low-Low in One Loop (2/4)

CCF	1.72E-04	Slave relays		
CCF	1.01E-04	Universal logic cards		
CCF	8.85E-05	Safeguards driver cards		
CCF	5.27E-05	Analog channels		
CCF	5.40E-06	118V AC power supply		
CCF	4.95E-06	Master relays		
CCF	3.60E-06	48V DC power supply		
CCF	3.60E-06	15V DC power supply		
1.	4.06E-06	-MRCMAFW	MRDMAFW	SGDCF
2.	4.06E-06	MRCMAFW	-MRDMAFW	SGDDF
3.	3.23E-06	-TATAFW	TBTAFW	SGDCF
4.	3.23E-06	TATAFW	-TBTAFW	SGDDF
5.	3.23E-06	-SRC2T	SRD2T	SGDCF
6.	3.23E-06	SRC2T	-SRD2T	SGDDF
7.	3.23E-06	-SRC1T	SRD1T	SGDCF
8.	3.23E-06	SRC1T	-SRD1T	SGDDF
9.	3.13E-06	SGDCF	SGDDF	
10.	2.64E-06	-MRCMAFW	MRDMAFW	UL313CF
11.	2.64E-06	-MRCMAFW	MRDMAFW	UL316CF
12.	2.64E-06	MRCMAFW	-MRDMAFW	UL313DF
13.	2.64E-06	MRCMAFW	-MRDMAFW	UL316DF
14.	2.10E-06	-TATAFW	TBTAFW	UL313CF
15.	2.10E-06	-TATAFW	TBTAFW	UL316CF
16.	2.10E-06	TATAFW	-TBTAFW	UL313DF
17.	2.10E-06	TATAFW	-TBTAFW	UL316DF
18.	2.10E-06	-SRC2T	SRD2T	UL313CF
19.	2.10E-06	-SRC2T	SRD2T	UL316CF
26.	2.10E-06	SRC2T	-SRD2T	UL313DF
27.	2.10E-06	SRC2T	-SRD2T	UL316DF
28.	2.10E-06	-SRC1T	SRD1T	UL313CF
29.	2.10E-06	-SRC1T	SRD1T	UL316CF
30.	2.10E-06	SRC1T	-SRD1T	UL313DF
31.	2.10E-06	SRC1T	-SRD1T	UL316DF

See Table 8.24 for descriptions of basic event identifiers.

Table 8.23 Dominant Cutsets for Signal Failure - Combined Case SSPS Reactor Trip: Pressurizer Pressure High (2/4)

CCF	6.23E-05	Analog channels			
CCF	5.06E-05	Universal logic cards			
CCF	2.93E-05	Undervoltage driver cards			
CCF	3.60E-06	15V DC power supply			
CCF	3.18E-06	Reactor trip breakers			
1.	3.91E-06	UL416BF	-RTBBT	-RTBBM	RTBAM
2.	3.91E-06	UL416AF	RTBBM	-RTBAT	-RTBAM
3.	3.44E-06	UVDBF	-RTBBT	-RTBBM	RTBAM
4.	3.44E-06	UVDAF	RTBBM	-RTBAT	-RTBAM
5.	2.61E-06	-TBTRT	-TBMRT	TAMRT	UL416BF
6.	2.61E-06	TBMRT	-TATRT	-TAMRT	UL416AF
7.	2.30E-06	-TBTRT	-TBMRT	TAMRT	UVDBF
8.	2.30E-06	TBMRT	-TATRT	-TAMRT	UVDAF
9.	1.57E-06	UL416BF	-RTBBT	-RTBBM	RTBAT
10.	1.57E-06	UL416AF	RTBBT	-RTBAT	-RTBAM
11.	1.38E-06	UVDBF	-RTBBT	-RTBBM	RTBAT
12.	1.38E-06	UVDAF	RTBBT	-RTBAT	-RTBAM
13.	1.32E-06	UL416BF	UL416AF		
14.	1.16E-06	UVDBF	UL416AF		
15.	1.16E-06	UL416BF	UVDAF		
16.	1.15E-06	RTOPER1	UL416BF		
17.	1.15E-06	RTOPER2	UL416AF		
18.	1.05E-06	-TBTRT	-TBMRT	TATRT	UL416BF
19.	1.05E-06	TBTRT	-TATRT	-TAMRT	UL416AF
20.	1.02E-06	UVDBF	UVDAF		
21.	1.01E-06	RTOPER1	UVDBF		
22.	1.01E-06	RTOPER2	UVDAF		
23.	9.19E-07	-TBTRT	-TBMRT	TATRT	UVDBF
24.	9.19E-07	TBTRT	-TATRT	-TAMRT	UVDAF
25.	1.68E-07	TBMRT	RTAF	-TATRT	-TAMRT
26.	1.68E-07	RTBF	-TBTRT	-TBMRT	TAMRT
27.	1.23E-07	15VDCB	-RTBBT	-RTBBM	RTBAM
28.	1.23E-07	15VDCA	RTBBM	-RTBAT	-RTBAM

See Table 8.24 for descriptions of basic event identifiers.

Table 8.24 Descriptions of Basic Event Identifiers Listed in Tables 8.21 through 8.23

CCF - common cause failure

15VDCx - 15V DC power supply faults in train x

MRxMAFW - auxiliary feedwater master relay x in maintenance

MRxMSI - safety injection master relay x in maintenance

RTxF - reactor trip breaker in train x fails

RTBxM - train x reactor trip breaker in maintenance

RTBxT - train x reactor trip breaker in test

RTOPER# - operator error

SRx#T - slave relay x# in test

SGDxF - safeguards driver card x fails

TxTAFW - auxiliary feedwater train x in test

TxMRT - reactor trip train x in maintenance

TxTRT - reactor trip train x in test

TxTSI - safety injection train x in test

UL###xF - universal logic card ### in train x fails (### refers to card number)

UVDxF - undervoltage driver card in train x fails

"-" - not symbol (example: -TBT = train B not in test)

8.3.5 Comparison to WCAP-14333 and NUREG/CR-5500

As previously discussed, this analysis provides several changes to the fault trees modeling the unavailability of the reactor trip and engineered safety feature actuation signals. This analysis also uses improved component failure rate data and common cause failure parameters. These changes provide improved representation of signal unavailabilities. Comparison of these unavailability values to similar values from other studies provides credibility to the analysis in demonstrating that analysis is not overly conservative or optimistic with regard to the ability of the RPS to reliably develop such signals. Table 8.25 provides such a comparison of signal unavailabilities. This table provides a comparison of signal unavailabilities for the results in this WCAP with the results in WCAP-14333 and NUREG/ CR 5500. Signal unavailabilities are provided for representative SI, AFW pump start, and reactor trip signals for the SSPS. WCAP-14333 STIs and CTs (referred to as the base case in this WCAP) is the basis.

This shows that the unavailability values for the SI and AFWPS signals between the current study and WCAP-14333 are similar. In general, this current study provides lower unavailability values which is primarily related to the improved component failure probability data used in the assessment. Most of the data, including the CCF parameters, is now based on nuclear industry specific experience, as opposed to the generic data used in WCAP-14333.

With regard to reactor trip signals, the unavailability values calculated in this study compare favorably with the values in NUREG/CR-5500. This current study also compares favorably with the WCAP-14333 analysis for RT signals from diverse sources. The only values that are not comparable are those for RT from diverse signals with operator action between this current study and WCAP-14333. The large difference in these values is due to the reactor trip breaker common cause failure contribution and failure probability of the reactor trip breakers. The values for the parameters used in this study are based on NUREG/CR-5500, whereas the values used in WCAP-14333 are conservative generic values.

Table 8.25 Comparison of Signal Unavailabilities with Other Studies

Signal	Current Study	WCAP-14333	NUREG/CR-5500
SI, 2/4 logic with OA	6.05E-04	7.24E-04	N/A
SI, 2/4 logic	8.96E-04	1.43E-03	N/A
SI, 2/3 logic with OA	6.07E-04	7.57E-04	N/A
SI, 2/3 logic	1.12E-03	2.92E-03	N/A
AFWPS, 2/4 logic	3.41E-04	7.24E-04	N/A
AFWPS, 2/3 logic	5.40E-04	1.66E-03	N/A
RT, 2/4 logic, with OA	2.74E-06	1.98E-05	N/A
RT, 2/3 logic, with OA	4.96E-06	2.91E-05	N/A
RT, diverse signals	2.69E-05	3.23E-05	2.2E-05
RT, diverse signals, with OA	2.22E-06	1.80E-05	5.5E-06

8.4 RISK IMPACT ANALYSIS

The risk impact analysis requires the calculation of several parameters to be consistent with the Risk Informed Regulatory Guides. Risk parameters which need to be determined are:

- Impact on yearly core damage frequency
- Incremental conditional core damage probability
- Impact on yearly large early release frequency
- Incremental conditional large early release probability

The steps for quantifying the risk parameters using the Vogtle PRA model are defined in Section 8.1.3. In the Vogtle PRA, the ESFAS signals are included as part of the support systems model, primarily for safety injection actuation, or within some of the fault tree models for systems requiring automatic actuation by the ESFAS, such as auxiliary feedwater system and steamline isolation. The reactor trip signals were included in the event tree models as appropriate.

The approach used in this analysis simply substitutes the unavailability values calculated based on the WOG TOP signal unavailability models in Section 8.3, for the corresponding values in the Vogtle PRA model. These substitutions occur in the support system model, event trees, and fault trees as necessary. After the substitution, the model is re-quantified with the WESQT Computer Code (Reference 10) to determine the CDF, LERF, and accident sequences. WESQT is a software tool used to quantify event trees, summarize the event tree quantification results, and provide the results in terms of total core damage frequency, frequency by initiator, accident sequences, end state frequencies, and event tree top event impòrtances based on contribution to core damage frequency. This importance function is defined as:

Importance = (Σ(CDF of sequences with top event failure)/total CDF) x 100

The baseline case was initially quantified with the signal unavailabilities corresponding to the proposed case from WCAP-14333, shown in Table 8.7 as the Base Case. These were followed by quantifications with the signal unavailabilities for the seven cases defined in Section 8.3.1. The quantifications conservatively did not take any credit for potential trip reduction due to the implementation of the revised analog channel STIs in WCAP-10271.

The risk analysis only evaluated the impact of the changes for signals generated from the SSPS. As discussed in Section 8.3.4, the results of the SSPS unavailability analysis can be used to represent the results of the relay protection system unavailability analysis. Therefore, the risk analysis was completed only with the SSPS results and is considered to be representative of the results expected for the relay protection systems. This approach is consistent with the approach used in WCAP-14333.

Finally, the approach includes evaluations of the impact of the changes on risk for signals generated from 2 of 3 logic and 2 of 4 logic. The signal unavailability results presented in Section 8.3.4 are not significantly different for signals generated for 2 of 3 logic verses 2 of 4 logic, when diversity or additional operator actions to trip the plant or actuate safety features are considered. This difference is primarily important when the signal is generated from a single set of analog channels (one 2 of 3 set or one 2 of 4 set).

8.4.1 Accident Sequence Identification

The entire Vogtle PRA model was requantified as described in Section 8.1. It was not necessary to identify and modify the unavailabilities for specific accident sequences. As discussed in Section 8.1.3, any additional calculations required with respect to the protection system unavailabilities, such as crediting manual actuation of individual components for safety injection, were performed prior to the model quantification. An example is the additional calculation to account for the operator action to manually re-align and start the required ECCS components for safety injection if the automatic signal fails.

Table 8.26 shows the relationship of the reactor trip signal modeled to the initiating event and whether operator action for the reactor trip is included in the model. Table 8.27 presents similar information for the ESFAS signals modeled in the Vogtle PRA. Both tables represent the Vogtle PRA model, which was not changed for the risk analysis calculations.

8.4.2 Data Development

For the unavailabilities used in the risk impact analysis, several signal unavailabilities were combined with the failure of the operator to manually actuate the safety system. The failure probabilities for the operator actions are listed in Table 8.28.

Table 8.26 Sources of Reactor Trip Actuation Signals

Event	Reactor Trip Actuation Signal	Operation Action
Large LOCA	Not Required	--
Medium LOCA	Not Required	--
Small LOCA	Nondiverse	Yes
Steam Generator Tube Rupture	Nondiverse	Yes
Interfacing Systems LOCA	Not Required	--
Reactor Vessel Rupture	Not Required	--
Secondary Side Break Inside Containment	Nondiverse	Yes
Secondary Side Break Outside Containment	Nondiverse	Yes
Positive Reactivity Insertion	Diverse	Yes
Loss of Reactor Coolant Flow	Diverse	Yes
Loss of Main Feedwater Flow	Diverse	Yes
Partial Loss of Main Feedwater Flow	Diverse	Yes
Loss of Condenser	Diverse	Yes
Turbine Trip	Diverse	Yes
Reactor Trip	Generated by RPS	--
Spurious Safety Injection Signal	Diverse	Yes
Inadvertent Opening of a Steam Valve	Diverse	Yes
Primary System Transient	Diverse	Yes
Loss of Offsite Power	Not Required by RPS	--
Station Blackout	Not Required by RPS	--
Loss of Instrument Air	Diverse	Yes
Total Loss of Nuclear Service Cooling Water	Nondiverse	Yes
Loss of 125 VDC Bus	Diverse	Yes
Loss of Two 120V Vital AC Instrument Panels	Diverse	Yes

Table 8.27 Sources of Engineered Safety Features Actuation Signals

Safety Function	Event	Signal Actuation Source
Safety Injection	Large LOCA	Nondiverse signal
	Medium LOCA	Nondiverse signal, OA by SI switch on main control board
	Small LOCA	Nondiverse signal, OA by SI switch on main control board, OA of individual components
	Interfacing Systems LOCA	Nondiverse signal, OA by SI switch on main control board, OA of individual components
	SG Tube Rupture	Nondiverse signal, OA by SI switch on main control board, OA of individual components
	Secondary Side Breaks	Nondiverse signal, OA by SI switch on main control board, OA of individual components
Auxiliary Feedwater Pump Start	Events generating SI signal Transients	Pump actuation on SI signal Nondiverse signal, AMSAC, operator action
Main Feedwater Isolation	Secondary Side Breaks	Nondiverse signal
Steamline Isolation	Secondary Side Breaks	Nondiverse signal
Containment Spray Actuation	All events	Nondiverse signal
Containment Isolation	All events	From SI signal
Containment Cooling	All events	From SI signal

Table 8.28 Summary of Human Error Probabilities for Operator Actions Backing Up Actuation Signals

Operator Action	HEP (1)	Source
Reactor trip from the main control board trip switches	1E-02	Conservative estimate based on several IPEs
Reactor trip by interrupting power from the motor-generator sets given that the operator failed to trip by the control board switches	5E-01	Vogtle PRA (2)
Manually insert the control rods into the core given the previous operator actions to trip have failed	5E-01	Vogtle PRA (2)
Safety injection from the main control board switches	1E-02	Conservative estimate based on several IPEs
Safety injection by manual actuations of individual components	2E-03	Vogtle PRA (2)
Auxiliary feedwater pump start	2E-02	Vogtle PRA (2)

Notes:

1) HEP - Human Error Probability

2) Vogtle PRA - see Reference 13

8.4.3 Calculation of Risk Parameters

The risk parameters of core damage frequency and large early release frequency were calculated for each case. One set of calculations was performed for the 2 out of 3 signal logic and another was performed for the 2 out of 4 signal logic. The incremental conditional core damage probability was calculated for the 2 out of 3 signal logic for Case 7 (the proposed case). The incremental large early release probability was evaluated based on the equipment affected and the other risk parameter results. A brief description of the calculation or evaluation of each risk parameter and the results are presented in the following sections.

8.4.3.1 Core Damage Frequency Assessment

The Vogtle PRA signal and system unavailabilities affected by the change for a given case were revised and the model was requantified. CDF values were calculated for a base case and seven sensitivity cases for 2 out of 3 signal logic and 2 out of 4 signal logic. The calculated values for CDF are presented in Table 8.29. The 2 out of 3 logic results show the same trends as the 2 out of 4 logic results. The increases in CDF compared to the Base Case are small based on the Regulatory Guide 1.174 guidance of 1.0E-06 per year, with the exception of Case 4. Case 3 shows a risk improvement compared to the Base Case. This is because the improvement of the unavailability due to the less frequent testing was greater than the effect of increased failure probabilities associated with the less frequent testing. Case 7, which is the proposed case, has an increase of less than 1.0E-06 per year over the Base Case.

System importance values, calculated as described in Section 8.4, are presented in Tables 8.30 and 8.31. Table 8.30 presents the system importance values for the Base Case and Case 7 for the 2 out of 4 logic, and Table 8.31 presents the 2 out of 3 logic results. The results for both logic systems are similar. Comparing the Base Case to Case 7, the most significant change is the increased importance of the reactor trip system and the pressurizer PORVs and safety valves. The unavailability of the reactor trip system is increased for Case 7, and this results in an increase in the contribution of anticipated transients without scram sequences to the total plant core damage frequency. This increases the importance of the reactor trip system and the PORVs and safety valve top events.

8.4.3.2 Incremental Conditional Core Damage Probability Assessment

For the proposed AOT and STI changes, incremental conditional core damage probability calculations only apply to the reactor trip breakers because they are the only components for which the AOT is being extended. The conditional CDF calculations were performed for the AOT associated with Case 7, the proposed case.

The incremental conditional core damage probability is defined as:

> ICCDP = [(conditional CDF with subject equipment out of service)-(baseline CDF with nominal expected equipment unavailabilities)] x (duration of single AOT under consideration) (Reference 2)

The Vogtle PRA was requantified with the reactor trip top event unavailabilities (2 out of 3 logic) adjusted for one reactor trip breaker out of service. The conditional CDF is 7.07E-05 per year. The baseline CDF used in the calculation is the Base Case CDF of 5.05E-05 per year from Table 8.29. Two CTs are considered; 30 hours for maintenance and 4 hours for a test. The above equation becomes:

ICCDP = (7.07E-05/yr – 5.05E-05/yr) x 30 hrs/(8760 hrs/yr) = 6.92E-08, and
ICCDP = (7.07E-05/yr – 5.05E-05/yr) x 4 hrs/(8760 hrs/yr) = 9.22E-09

Both of the above calculated values are below 5E-07, which is considered very small for a single Technical Specification Completion Time (Reference 2).

8.4.3.3 Large Early Release Frequency Assessment

For each case quantified, endstates are generated for sequences above the quantification cutoff. The endstates contain information about the initiating event, timing of core damage, the containment isolation status, the pressure of the RCS, and the availability of the emergency core cooling, containment cooling, and containment spray systems. For a conservative estimation of LERF, the endstates representing containment bypass and containment isolation failure were summed. This is the same approach as described in the response to RAI 13 documented in WCAP-14333. The calculated values for LERF are presented in Table 8.32. The 2 out of 3 logic results show the same trends as the 2 out of 4 logic results. The increases in LERF compared to the Base Case are small based on the Regulatory Guide 1.174 guidance of 1.0E-07 per year, with the exception of Case 4. Case 3 shows a risk improvement compared to the Base Case. This is because the improvement of the unavailability due to the less frequent testing was greater than the effect of the increase in failure rates associated with the less frequent testing. Case 7, which is the proposed case, has an increase of less than 1.0E-07 per year over the Base Case.

8.4.3.4 Incremental Conditional Large Early Release Probability Assessment

Detailed calculations to determine the impact on incremental conditional large early release probability are not required. For the proposed AOT and STI changes, incremental large early release probability calculations only apply to the reactor trip breakers because they are the only components for which the AOT is being extended. Reactor trip breakers are used to mitigate core damage, not containment failure. Reactor trip breaker success or failure has no direct impact on the functioning of containment systems. Large releases are related to containment bypass events, containment isolation failures, and containment failures. Reactor trip breaker success or failure has no direct bearing on these functions. As shown previously, the extended reactor trip breaker AOT will result in a slight increase in frequency of some core damage sequences. Because the success or failure of the containment systems is independent of the reactor trip breakers, the LERF will increase only in direct proportion to the increased frequency of core damage sequences involving reactor trip breaker failures. Therefore, because the impact of the reactor trip breaker AOT increase on CDF and LERF is small and the ICCDP is acceptable, the ICLERP will also be acceptable.

An analysis was completed to address Request for Additional Information Number 11 in the NRC letter dated August 1, 2001, from M. L. Scott, NRC, to A. Drake, Westinghouse, Westinghouse Topical Report WCAP-15376, "Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactors Trip Breaker Test and Completion Times" (TAC No. MB0983) (see Appendix D). This analysis calculated the ICLERP for an RTB out of service. The ICLERP for an RTB out of service for a total time of 30 hours (a Completion Time of 24 hours plus 6 hours to reach Mode 3) is 2.42E-08 for corrective maintenance. and 2.41E-08 for preventive maintenance.

Table 8.29 Summary of Results by Core Damage Frequency

Case	Parameter Change	2/4 Logic			2/3 Logic		
		CDF (per year)	Change: Case to Base Case (per year)	Change: Case to Base Case (%)	CDF (per year)	Change: Case to Base Case (per year)	Change: Case to Base Case (%)
Base Case		5.05E-05	--	--	5.05E-05	--	--
Case 1	Analog Channels STI @ 6months	5.05E-05	1.00E-08	0.02	5.06E-05	4.00E-08	0.08
Case 2	Logic Cabinets STI @ 6 months	5.06E-05	1.90E-07	0.38	5.07E-05	1.80E-07	0.36
Case 3	Master Relays STI @ 6 months	5.01E-05	-3.50E-07	-0.69	5.02E-05	-3.50E-07	-0.69
Case 4	Reactor Trip Breakers STI @ 6 months	5.23E-05	1.88E-06	3.73	5.24E-05	1.88E-06	3.72
Case 5	Reactor Trip Breakers Maint. @ 30 hrs, Test Time @ 4 hrs	5.05E-05	1.00E-08	0.02	5.06E-05	1.00E-08	0.02
Case 6	Reactor Trip Breakers STI @ 4 months	5.14E-05	9.30E-07	1.84	5.15E-05	9.30E-07	1.84
Case 7	Combined Cases 1, 2, 3, 5, and 6 with Reactor Trip Breakers STI @ 4 months	5.13E-05	8.00E-07	1.59	5.14E-05	8.50E-07	1.68

Table 8.30 System (Top Event) Importance Summary: SSPS with 2 of 4 Logic

System	Importance Measure	
	Base Case	Case 7
4160 VAC Power	63.3 %	62.3 %
Auxiliary Feedwater	18.4 %	18.7 %
Nuclear Service Cooling Water	17.7 %	17.3 %
CB ESF Electrical Equipment Room HVAC	17.4 %	17.1 %
Condensate Feed	12.5 %	12.3 %
Essential Chilled Water System	10.1 %	9.9%
Turbine Driven AFW Pump	8.3%	8.2%
High Pressure Injection	7.3%	7.3%
High Pressure Recirculation	7.1%	7.0%
Containment Cooling Units	6.8%	6.8%
Engineered Safety Features	6.6%	6.0%
Component Cooling Water	4.9%	4.8%
Centrifugal Charging Pumps	3.8%	3.6%
Low Pressure Injection	3.7%	3.6%
Safety Injection Pumps	3.1%	3.0%
Low Pressure Recirculation	2.3%	2.2%
Reactor Trip	2.1%	4.1%
RWST Failure	1.9%	1.8%
480 VAC Buses Train A	1.6%	1.6%
Normal Chilled Water System	1.5%	1.4%
Hot Leg Recirculation	1.4%	1.3%
Normal Charging	1.0%	1.0%
PORVs and/or SVs Open	1.0%	1.9%
125 VDC Buses	0.9%	0.9%
Pressurizer PORVs	0.8%	0.8%

Table 8.31 System (Top Event) Importance Summary: SSPS with 2 of 3 Logic		
	Importance Measure	
System	Base Case	Case 7
4160 VAC Power	63.2%	62.1%
Auxiliary Feedwater	18.4%	18.7%
Nuclear Service Cooling Water	17.7%	17.3%
CB ESF Electrical Equipment Room HVAC	17.4%	17.1%
Condensate Feed	12.5%	12.3%
Essential Chilled Water System	10.0%	9.9%
Turbine Driven AFW Pump	8.3%	8.1%
High Pressure Injection	7.4%	7.5%
High Pressure Recirculation	7.1%	7.0%
Containment Cooling Units	6.9%	7.0%
Engineered Safety Features	6.8%	6.2%
Component Cooling Water	4.9%	4.8%
Centrifugal Charging Pumps	3.8%	3.6%
Low Pressure Injection	3.8%	3.8%
Safety Injection Pumps	3.1%	3.0%
Low Pressure Recirculation	2.3%	2.2%
Reactor Tnp	2.1%	4.1%
RWST Failure	1.9%	1.8%
480 VAC Buses Train A	1.6%	1.6%
Normal Chilled Water System	1.5%	1.4%
Hot Leg Recirculation	1.4%	1.3%
Normal Charging	1.0%	1.0%
PORVs and/or SVs Open	1.0%	1.9%
125 VDC Buses	0.9%	0.9%
Pressurizer PORVs	0.8%	0.8%

Table 8.32 Summary of Results by Large Early Release Frequency

		2/4 Logic			2/3 Logic		
Case	Parameter Change	LERF (per year)	Change: Case to Base Case (per year)	Change: Case to Base Case (%)	LERF (per year)	Change: Case to Base Case (per year)	Change: Case to Base Case (%)
Base Case		2.38E-06	--	--	2.44E-06	--	--
Case 1	Analog Channels STI @ 6 months	2.40E-06	1.55E-08	0.67	2.48E-06	3.43E-08	1.49
Case 2	Logic Cabinets STI @ 6 months	2.38E-06	2.45E-09	0.11	2.45E-06	2.34E-09	0.10
Case 3	Master Relays STI @ 6 months	2.27E-06	-1.14E-07	-4.95	2.27E-06	-1.76E-07	-7.62
Case 4	Reactor Trip Breakers STI @ 6 months	2.49E-06	1.09E-07	4.74	2.55E-06	1.09E-07	4.74
Case 5	Reactor Trip Breakers Maint. @ 30 hrs, Test Time @ 4 hrs	2.38E-06	1.66E-09	0.07	2.44E-06	6.25E-10	0.03
Case 6	Reactor Trip Breakers STI @ 4 months	2.43E-06	5.37E-08	2.33	2.50E-06	5.28E-08	2.29
Case 7	Combined Cases 1, 2, 3, 5, and 6 with Reactor Trip Breakers STI @ 4 months	2.41E-06	3.09E-08	1.34	2.50E-06	5.68E-08	2.47

8.4.4 Comparison to Previous STI and CT Parameters

This analysis quantifies the impact on CDF of the STI and CT changes being considered using the STIs and CTs in WCAP-14333 as the base case. Table 8.33 provides the impact on CDF with respect to the pre-TOP STIs and CTs for the SSPS. The pre-TOP parameters are provided on Table 1.1. This comparison credits the expected reduction in reactor trips due to the reduced analog channel testing related to the analog channel STI extension from monthly to quarterly evaluated in WCAP-10271. The impact on CDF for the changes from pre-TOP to WCAP-14333 are from Reference 6. These are added to the current impact on CDF to obtain an estimate of the overall impact on CDF of all the RPS and ESFAS STI and CT changes previously approved by the NRC in addition to these currently being requested. This information is provided for two-out-of-four and two-out-of-three channel logic. The calculated impact on CDF for both logic requirements is small.

Table 8.33 Impact of Cumulative STI and CT Changes on Core Damage Frequency

Case	2/4 Logic	2/3 Logic
CDF Impact: Pre-TOP to WCAP-14333	-2.3E-07/yr	2.4E-07/yr
CDF Impact: WCAP-14333 to Current Request	8.0E-07/yr	8.5E-07/yr
CDF Impact: Pre-TOP to Current Request	5.7E-07/yr	1.1E-06/yr

8.5 TIER 2: AVOIDANCE OF RISK-SIGNIFICANT PLANT CONDITIONS

The objective of the second tier, which is applicable to CT extensions, is to provide reasonable assurance that risk-significant plant equipment outage configurations will not occur when equipment is out of service. If risk-significant configurations do occur, then enhancements to Technical Specifications or procedures, such as limiting unavailability of backup systems, increased surveillance frequencies, or upgrading procedures or training, can be made that avoid, limit, or lessen the importance of these configurations.

Restrictions on concurrent removal of certain equipment when an RTB is out of service are identified in the following:

- The probability of failing to trip the reactor on demand will increase when an RTB is removed from service; therefore, systems designed for mitigating an ATWS event should be maintained available. RCS pressure relief, auxiliary feedwater flow (for RCS heat removal), AMSAC, and turbine trip are important alternate for ATWS mitigation. Therefore, activities that degrade the availability of the auxiliary feedwater system, RCS pressure relief system (pressurizer PORVs and safety valves), AMSAC, or turbine trip should not be scheduled when an RTB is out of service.

- Due to the increased dependence on the available reactor trip train when one logic cabinet is removed from service, activities that degrade other components of the RPS, including master relays or slave relays and activities that cause analog channels to be unavailable, should not be scheduled when a logic cabinet is unavailable.

- Activities on electrical systems (e.g., AC and DC power) that support the systems or functions listed in the first two bullets above should not be scheduled when a RTB is unavailable.

8.6 TIER 3: RISK-INFORMED PLANT CONFIGURATION CONTROL AND MANAGEMENT

The objective of the third-tier is to ensure that the risk impact of out-of-service equipment is evaluated prior to performing any maintenance activity. As stated in RG-1.174, "a viable program would be one that is able to uncover risk-significant plant equipment outage configurations as they evolve during real-time, normal plant operation." The third-tier requirement is an extension of the second-tier requirement, but addresses the limitation of being able to identify all possible risk-significant plant configurations in the second-tier evaluation.

Addressing third-tier requirements is outside the scope of this document. This will be addressed on a utility specific basis when the changes in this WCAP are implemented at each plant and will be addressed through each plant's Maintenance Rule Program ((a)(4) requirement).

8.7 POTENTIAL SHUTDOWN RISK AVOIDED WITH EXTENDED COMPLETION TIME

One of the benefits of extended CTs is the risk associated with avoiding a plant shutdown and the ensuing startup. Extended CTs will help utilities avoid plant shutdowns by allowing additional time to complete repair activities and restore parameters to within limits. Extended CTs will also help utilities to avoid requests for discretionary enforcement to remain at-power when the time to complete a repair or a restoration activity exceeds, or will exceed, the current CT.

A previous study (Reference 6) examined the risk associated with a plant shutdown and the subsequent startup. The Reference 6 study divided the plant shutdown into two phases; the power reduction phase in Mode 1 and the changes in operating modes after the reactor is tripped. Similarly, the plant startup was divided into two phases; the changes in operating modes prior to achieving criticality and the power increase that occurs in Mode 1 after the control rods are pulled. This referenced study only considered the risk associated with the power reduction and power increase phases of the shutdown and startup.

Based on the plant operating data presented in Reference 6, the probability of tripping the reactor during the power reduction phase of a plant shutdown is 0.088; and the probability of tripping the reactor during the power ascension phase of a plant startup is 0.068. This study provides the conditional CDF, conditional on a transient event, such as a partial loss of main feedwater occurring, to be 3E-06. Therefore, the probability of core damage based on this conditional core damage frequency and probability of inducing a transient event during the shutdown or startup is:

$$\text{CDP} = (0.088 + 0.068) \times 3\text{E-}06 = 4.7\text{E-}07$$

This value is comparable to the expected CDF change related to the RTB CT increase presented in Table 8.29.

9.0 IMPACT ON DEFENSE-IN-DEPTH AND SAFETY MARGINS

The traditional engineering considerations need to be addressed also. These include defense-in-depth and safety margins. The fundamental safety principles on which the plant design is based cannot be compromised. Design basis accidents are used to develop the plant design. These are a combination of postulated challenges and failure events that are used in the plant design to demonstrate safe plant response. Defense-in-depth, the single failure criterion, and adequate safety margins may be impacted by the proposed change and consideration needs to be given to these elements.

9.1 IMPACT ON DEFENSE-IN-DEPTH

The proposed change needs to meet the defense-in-depth principle which consists of a number of elements. These elements and the impact of the proposed change on these elements follow:

- A reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation is preserved

  The proposed STI changes to the RTS and ESFAS and the proposed change to the RBT CT have only a small calculated impact on CDF and LERF. The AOT and STI changes to the RTB only impact CDF and have no impact on containment integrity. The STI changes to the analog channels, logic cabinets, and master relays have small calculated impacts on both CDF and LERF. These changes to not degrade core damage prevention at the expense of containment integrity, nor do these changes degrade containment integrity at the expense of core damage prevention. The balance between prevention of core damage and prevention of containment failure is maintained. Consequence mitigation remains unaffected by the proposed changes. Furthermore, no new accident or transients are introduced with the requested change, and the likelihood of an accident or transient is not impacted. No new activities on the RPS will be performed at-power that could lead to potentially new transient events. Conversely, the increase in STIs could potentially lead to a reduction in the likelihood of a test induced transient or accident. This remains an unquantified benefit of the STI changes.

- Over-reliance on programmatic activities to compensate for weaknesses in plant design.

  The plant design will not be changed with these proposed changes. All safety systems, including the RPS, will still function in the same manner with the same signals available to trip the reactor and initiate ESF functions, and there will be no additional reliance on additional systems, procedures, or operator actions. The calculated risk increase for these changes is very small and additional control processes are not required to be put into place to compensate for any risk increase.

- System redundancy, independence, and diversity are maintained commensurate with the expected frequency and consequences of challenges to the system.

  There is no impact on the redundancy, independence, or diversity of the RPS or of the ability of the plant to respond to events with diverse systems. The RPS is a diverse and redundant system and will remain so. There will be no change to the signals available to trip the reactor or initiate

ESF functions. The RPS is a highly reliable system and will remain so after these proposed changes. The RPS is backed up by highly trained operators (and proceduralized actions) who will still be available to perform actions in the extremely rare occurrence of RPS failure. In addition, the RTS is backed up by AMSAC signal to start auxiliary feedwater and trip the turbine in conjunction with RCS pressure mitigation via the pressurizer safety valves and relief valves. The proposed changes have no impact on this alternate approach to ATWS mitigation. In fact, Tier 2 and 3 requirements place limitations on having the RTBs and components of ATWS mitigation system out of service similtaneously.

- Defenses against potential common cause failures are maintained and the potential for introduction of new common cause failure mechanisms is assessed.

  Defenses against common cause failures are maintained. The extensions requested are not sufficiently long to expected new common cause failure mechanisms to arise. In addition, the operating environment for these components remains the same so, again, new common cause failure modes are not expected. In addition, backup systems and operator actions are not impacted by these changes; and there are no common cause links between the RPS and these backup options. Furthermore, the RTB CT and bypass time increases are not requested to perform additional test and routine maintenance activities while at-power. Such activities will continue to be completed as currently required. Therefore, no new potential common cause failure mechanisms have been introduced.

- Independence of barriers is not degraded.

  The barriers protecting the public and the independence of these barriers are maintained. With the extended STIs and CTs, it is not expected that utilities will have multiple systems out service simultaneously that could lead to degradation of these barriers and an increase in risk to the public.

- Defenses against human errors are maintained.

  No new operator actions related to the STI extensions or the CT extension are required. No additional operating, maintenance, or test procedures have been introduced or modified due to these changes and no new at-power test or maintenance activities are expected to occur as a result of these changes. The plant will continue to be operated and maintained as before. With the CT increase, the plant can be maintained at-power longer to complete repair activities on the RTBs and with the STI increases fewer surveillance tests will need to be completed at-power which will reduce the potential for test induced reactor trips and safety system actuations. This represents a risk benefit, that is, a reduction in risk.

9.2 IMPACT ON SAFETY MARGINS

The safety analysis acceptance criteria as stated in the FSAR is not impacted by this change. Redundant RPS trains will be maintained. Diversity with regard to signals to provide reactor trip and actuation of engineered safety features will also be maintained. The proposed changes will not allow plant operation in a configuration outside the design basis. All signals credited as primary or secondary and all operator actions credited in the accident analysis will remain the same.

10.0 CONCLUSIONS

The following presents the conclusions of this study based on the analysis and results discussed in the previous sections. It is recommended based on these conclusions, that the CT for the RTBs and the STIs for the analog channels, logic cabinets, RTBs, and master relays (SSPS only) be increased to the values proposed in Tables 4.1 and 4.2.

1. The proposed changes to the STIs and the RBT CT and bypass times have an insignificant impact on plant safety. This conclusion applies to signals generated by the solid state protection system and the relay protection system. As seen in Section 8.4, the increase in core damage frequency for all changes is small, and meets the criteria in RG 1.174. In addition, as seen in Section 8.4, the ICCDP for the RTB CT and bypass time changes meet the acceptance criteria in RG 1.177.

2. The risk averted by eliminating a plant shutdown and restart due to the proposed CT change, offsets the increase in risk of the proposed change due to increased signal unavailability while at-power.

3. The proposed changes being considered have a minor impact on the availability of the RT and ESF actuation signal. This is particularly evident for functions that are backed-up by either diverse actuation signals or operator actions.

4. The impact of the proposed changes on signal unavailability for the SSPS can be used to represent the impact of the changes on signals generated by relay protection systems.

5. One of the strengths of the reactor protection system is the ability of diverse signals and operator actions to initiate reactor trip and safety system actuations to mitigate initiating events. This diversity has been credited in this study.

6. The importance of the reactor trip and engineered safety features actuation signals are relatively low, and remain low with implementation of the proposed CT and bypass time changes.

7. Reactor trips and ESF actuations occur during test and maintenance activities. This indicates that these activities should be completed with caution and significant time should be available, and that reducing the number of these activities will reduce the potential for these types of trips and actuations.

11.0 IMPLEMENTATION OF THE PROPOSED TECHNICAL SPECIFICATION CHANGES

The analysis presented and discussed in the previous sections recommends the following:

1. Incorporate the CT and bypass time for the RTBs provided in Tables 4.1 and 4.2 into the RTS and ESFAS Instrumentation Technical Specifications.

2. Incorporate the STIs provided in Tables 4.1 and 4.2 into the RTS and ESFAS Instrumentation Technical Specifications.

Implementation of these proposed changes into the Standard Technical Specifications for Westinghouse Plants (NUREG-1431, Rev. 1) is shown in Appendix B. All of these changes are applicable to plants with NUREG-0452 and custom Technical Specifications.

Depending on the plant protection system design, some of the actuation logic and master relays associated with the Containment Purge and Exhaust Isolation Instrumentation (3.3.6) and CREFS Actuation Instrumentation (3.3.7) Technical Specifications may be processed through the Relay or Solid State Protection System. Since the STIs for the actuation logic and master relays of the ESFAS Instrumentation were justified to be relaxed in this report, these STI relaxations are also applicable to the actuation logic and master relays for all signals processed through the Relay or Solid State Protection System.

The STI for the source range neutron flux Channel Operational Test (COT) in the RTS Instrumentation (3.3.1) Technical Specification was justified to be relaxed in this report. Since this source range neutron flux channel is also used for the BDPS in Technical Specification 3.3.9, the STI relaxation is also applicable to that STI.

These recommendations are applicable to all the signals evaluated in WOG TOP for both solid state and relay protection systems (see Tables 3.2-2 and 3.2-3 in Reference 4 and Tables 3.1-2 and 3.1-3 in Reference 5 for a complete listing of the signals evaluated in previous WOG programs related to RPS instrumentation). The results are also applicable to those signals not specifically evaluated in the TOP analysis, but shown to be applicable through subsequent evaluations. These include:

- Reactor trip on steam generator level low-low with time delay

- Auxiliary feedwater pump start on steam generator level low-low with time delay

- Auxiliary feedwater suction transfer on suction pressure low

- Feedwater isolation on main steam valve vault room water level high

- Feedwater isolation on low reactor coolant system T_{avg} coincident with reactor trip

- Automatic switchover to containment sump on refueling water storage tank level low-low

- Semi-automatic switchover to containment emergency sump on RWST level low-low coincident with SI

- Automatic switchover to containment sump on RWST level low-low coincident with SI and containment sump level high

In addition, these results are applicable to any signals utilities have independently shown to be encompassed by the WOG TOP evaluation during plant specific implementation of the WCAP-10271 and WCAP-14333 Technical Specification changes.

This analysis and results only considered analog channels. But the results are also applicable to digital systems as justified by utilities previously implementing WOG TOP with the Eagle 21 process protection system and approved by the NRC.

12.0 REFERENCES

1. Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," July 1998.

2. Regulatory Guide 1.177, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications," August 1998.

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

4. "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System, Supplement 1," WCAP-10271, Supplement 1-P-A, May 1986.

5. "Evaluation of Surveillance Frequencies and Out of Service Times for the Engineered Safety Features Actuation System," WCAP-10271-P-A, Supplement 2, Revision 1.

6. "Probabilistic Risk Analysis of the RPS and ESFAS Test Times and Completion Times," WCAP-14333-P-A, Rev. 1, October 1998.

7. "Reliability Study: Westinghouse Reactor Protection System, 1984-1995," NUREG/CR-5500, Vol. 2, December 1998.

8. "Standard Technical Specifications, Westinghouse Plants, Bases (Section 2.0-3.3)," NUREG-1431, Vol. 2, Rev. 1.

9. "WesSAGE Code System User Manual," WCAP-14041, May 1994.

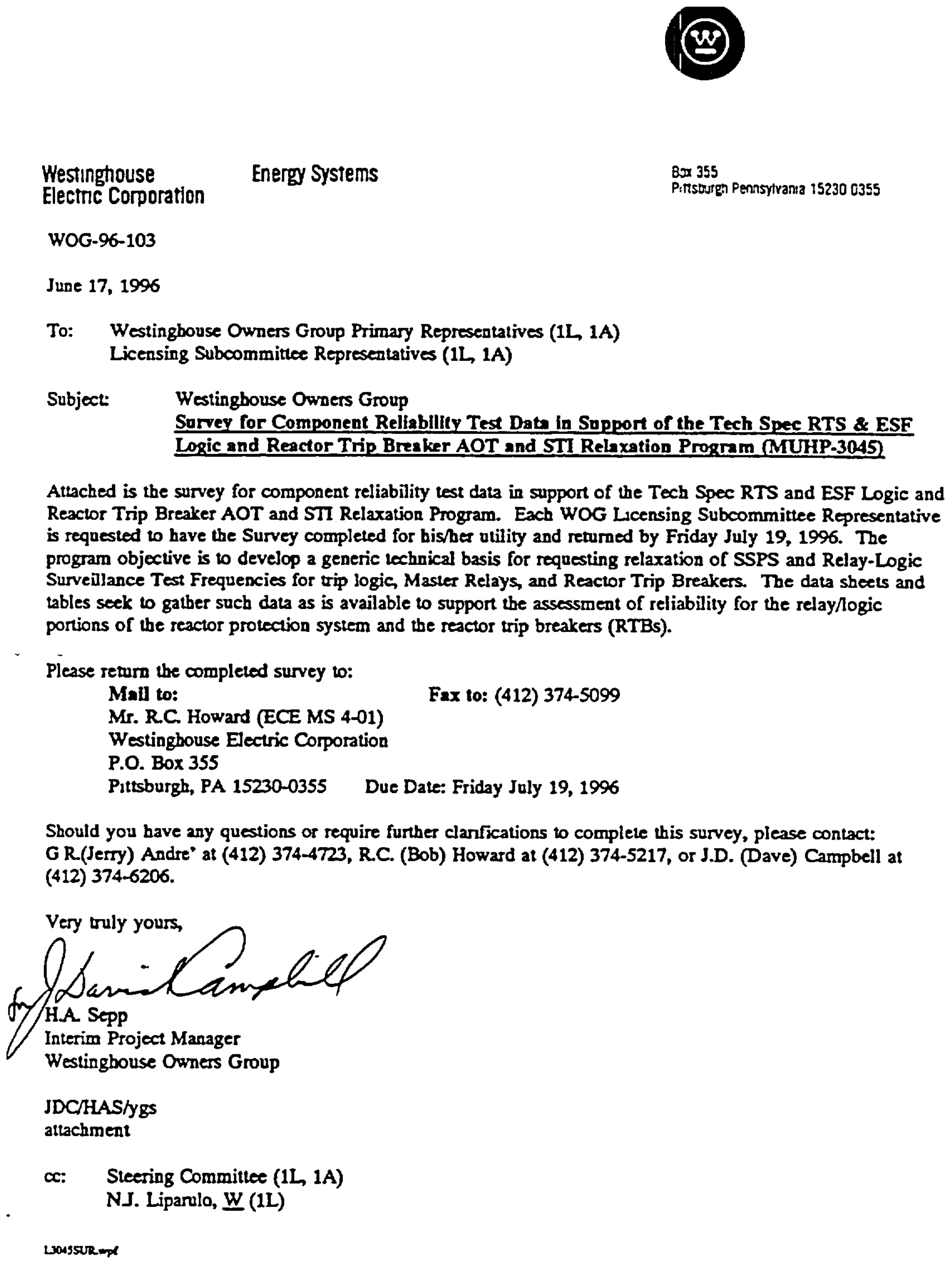
10. "Event Tree Development and Quantification System User Manual," WCAP-13199.

11. WOG-96-103, "Survey for Component Reliability Test Data in Support of the Tech Spec RTS & ESF Logic and Reactor Trip Breaker AOT and STI Relaxation Program (MUHP-3045)," June 17, 1996.

12. "Individual Plant Examination Report in Response to Generic Letter 88-20," Vogtle Electric Generating Station, November 1992.

APPENDIX A

Westinghouse letter: WOG-96-103, "Survey for Component Reliability Test Data in Support of the Tech Spec RTS and ESF Logic and Reactor Trip Breaker AOT and STI Relaxation Program (MUHP-3045)".



Westinghouse Electric Corporation

Energy Systems

Box 355
Pittsburgh Pennsylvania 15230 0355

WOG-96-103

June 17, 1996

To: Westinghouse Owners Group Primary Representatives (1L, 1A)
Licensing Subcommittee Representatives (1L, 1A)

Subject: Westinghouse Owners Group
Survey for Component Reliability Test Data in Support of the Tech Spec RTS & ESF Logic and Reactor Trip Breaker AOT and STI Relaxation Program (MUHP-3045)

Attached is the survey for component reliability test data in support of the Tech Spec RTS and ESF Logic and Reactor Trip Breaker AOT and STI Relaxation Program. Each WOG Licensing Subcommittee Representative is requested to have the Survey completed for his/her utility and returned by Friday July 19, 1996. The program objective is to develop a generic technical basis for requesting relaxation of SSPS and Relay-Logic Surveillance Test Frequencies for trip logic, Master Relays, and Reactor Trip Breakers. The data sheets and tables seek to gather such data as is available to support the assessment of reliability for the relay/logic portions of the reactor protection system and the reactor trip breakers (RTBs).

Please return the completed survey to:

Mail to: **Fax to:** (412) 374-5099
Mr. R.C. Howard (ECE MS 4-01)
Westinghouse Electric Corporation
P.O. Box 355
Pittsburgh, PA 15230-0355 Due Date: Friday July 19, 1996

Should you have any questions or require further clarifications to complete this survey, please contact: G R.(Jerry) Andre' at (412) 374-4723, R.C. (Bob) Howard at (412) 374-5217, or J.D. (Dave) Campbell at (412) 374-6206.

Very truly yours,

for J David Campbell

H.A. Sepp
Interim Project Manager
Westinghouse Owners Group

JDC/HAS/ygs
attachment

cc: Steering Committee (1L, 1A)
N.J. Liparulo, W (1L)

L3045SUR.wpf

COMPONENT RELIABILITY TEST DATA SHEET

WOG SURVEY DATA SHEETS

for MUHP-3045

1. Plant Name: ______________________________ Unit #: __________

2. Reactor Trip and Emergency Safeguard actuations are initiated from the (check one):

   ___ a Relay Logic Cabinets
   Please complete and return Sections 1 and 3 (disregard Section 2)

   ___ b. Solid State Protection System (SSPS)
   Please complete and return Sections 2 and 3 (disregard Section 1)

3. Type of Reactor Trip Breakers:

   ___ a. Westinghouse DB-50

   ___ b. Westinghouse DS-416

   ___ c. Other, please specify manufacturer and model:
   ____

Section 3 applies to all RTB makes and models. Please complete and return.

Mail to: Bob Howard (ECE MS 4-01)
(post office) Westinghouse Energy Center
P.O. Box 355
Pittsburgh, PA 15230-0355

(Fed Ex. to): 4350 Northern Pike
Monroeville, Pa., 15146

COMPONENT RELIABILITY TEST DATA SHEET

Section 1: Relay Logic Cabinets

Plant Name: ______________________________ Unit: ______

1-1. List relay types used as input relays:

No.	Manufacturer	Model	Quantity

1-2. List the relays types used as master relays:

No.	Manufacturer	Model	Quantity

1-3. List the timers or time delay relays used.

No.	Manufacturer	Model	Quantity	Timer/TD relay

COMPONENT RELIABILITY TEST DATA SHEET

1-4. List any general or large-scale replacements of power supplies, relays, or other components for the system. (When the new components are the same manufacturer and model, this is a "replacement in kind")

No.	Date	Component Description./Model	Replace d in kind?	If not replaced in kind, replacement type is:
			Yes No	
			Yes No	
			Yes No	
			Yes No	
			Yes No	
			Yes No	
			Yes No	
			Yes No	

1-5. List tests which impact the Relay-Logic Cabinet relays/components. The list should include all procedures which cause actuation of the components or collect data indicative of the component condition or environment. The test period should be on a per-component basis (enter "NO" if not periodic). Test Duration is the time the protection cabinet is out of service for the test. Describe the purpose/result of test (relay actuates, dry contact test, etc).

No.	Procedure ID No.	Test Period	Test Duration	Description of test purpose/result

COMPONENT RELIABILITY TEST DATA SHEET

1-6 Routine Testing of Similar Equipment

		YES	NO
a)	Are all components that perform the same function tested at the same period?		
b)	If "No", explain. Cite item number(s) from table above.		

1-7. Routine maintenance/surveillance programs inspect for:

		YES	NO
a)	Operation?		
b)	Condition of contacts?		
c)	Changes in appearance (color, texture)?		
d)	In-Cabinet "housekeeping"?		

1-8 Have "Failures" been observed in the Relay-Logic cabinets relays?

		YES	NO
a)	During testing?		
b)	In-service under normal conditions?		
c)	In-service under abnormal conditions?		
d)	Complete Table 2 (attached), listing all relays in the trip channel up to the final actuated device.		

1-9 Have "Failures" of the logic cabinet circuit boards or power supplies been observed?

		YES	NO
a)	During testing?		
b)	In-service under normal conditions?		
c)	In-service under abnormal conditions?		
d)	Complete Table 2 (attached), listing all circuit boards and power supplies.		

COMPONENT RELIABILITY TEST DATA SHEET

1-10 Cabinet Temperature Monitoring

		YES	NO
a)	Is temperature monitored and controlled in the area of the Relay-Logic cabinets (e.g., via Class 1E HVAC)?		
b)	If yes, what is the control setpoint for cooling?		°F
c)	If yes to a) what is the control setpoint for heating?		°F
d)	Describe the approximate location of temperature monitor relative to logic cabinet:		

1-11 Cabinet Temperature Data:

		YES	NO
a)	Are in-cabinet temperatures during normal operation known?		
b)	Are in-cabinet temperatures monitored routinely?		
c)	Were in-cabinet temperatures recorded on a one-time basis?		
d)	Have thermographic images of the cabinets been taken?		
e)	Provide what temperature data is available by completing Table 3.		

1-12 Please identify person(s) to be contacted if clarification of the above information is necessary.

Name: ______________________________ Phone No.: _______________

Name: ______________________________ Phone No.: _______________

Mail to: Bob Howard (ECE MS 4-01)
(post office) Westinghouse Energy Center
P.O. Box 355
Pittsburgh, PA 15230-0355

(Fed Ex. to): 4350 Northern Pike
Monroeville, Pa., 15146

COMPONENT RELIABILITY TEST DATA SHEET

Section 2: Solid State Protection System (SSPS)

Plant Name: ______________________________ Unit: _______

2-1. List relay types used as input relays:

No.	Manufacturer	Model	Quantity

2-2 List the relays types used as master relays:

No.	Manufacturer	Model	Quantity

2-3 List the number of each of the following circuit board types:

No.	Mnemonic	Name	Quantity
		Universal Logic Card	

COMPONENT RELIABILITY TEST DATA SHEET

2-4 List any general or large-scale replacements of power supplies, circuit boards, input or master relays, or other components for the system.				
No.	Date	Component Description./Model	Replaced in kind?	If not replaced in kind, replacement type is:
			Yes No	
			Yes No	
			Yes No	
			Yes No	
			Yes No	
			Yes No	

2-5 List tests which impact the SSPS input relays, circuit cards and master relay. The list should include all procedures which cause actuation of the components or collect data indicative of the component condition or environment. The test period should be on a per-component basis (enter "NO" if not periodic). Test Duration is the time the protection cabinet is out of service for the test. Describe the purpose/result of test (actuation logic tested, relay actuates, dry contact test, etc.).

No.	Procedure ID No.	Test Period	Test Duration	Description of test purpose/result

COMPONENT RELIABILITY TEST DATA SHEET

2-6	Routine Testing of Similar Equipment	YES	NO
a)	Are all components that perform the same function tested at the same period?		
b)	If "No", explain. Cite item number(s) from table above.		

2-7.	Routine maintenance/surveillance programs inspect for:	YES	NO
a)	Operation?		
b)	Condition of contacts?		
c)	Changes in appearance (color, texture)?		
d)	In-Cabinet "housekeeping"?		

2-8	Have "Failures" been observed in the SSPS input relays, circuit boards, power supplies or master relays	YES	NO
a)	During testing?		
b)	In-service under normal conditions?		
c)	In-service under abnormal conditions?		
d)	Complete Table 2 (attached), listing all input and master relays.		

2-9	Have "Failures" been observed in the SSPS circuit boards or power supplies	YES	NO
a)	During testing?		
b)	In-service under normal conditions?		
c)	In-service under abnormal conditions?		
d)	Complete Table 2 (attached), listing all circuit boards and power supplies.		

COMPONENT RELIABILITY TEST DATA SHEET

e)	Also, please attach a descriptive summary of any incidents where components in the Safeguards Test Cabinet (SGTC) have caused inadvertent actuations or plant trips during testing. Include reference to applicable plant documents or LERs

2-10 Cabinet Temperature Monitoring

		YES	NO
a)	Is temperature monitored and controlled in the area of the SSPS cabinets (e.g., via Class 1E HVAC)?		
b)	If yes, what is the control setpoint for cooling?		°F
c)	If yes to a) what is the control setpoint for heating?		°F
d)	Describe the approximate location of temperature monitor relative to SSPS:		

2-11 Cabinet Temperature Data:

		YES	NO
a)	Are in-cabinet temperatures during normal operation known?		
b)	Are in-cabinet temperatures monitored routinely?		
c)	Were in-cabinet temperatures recorded on a one-time basis?		
d)	Have thermographic images of the cabinets been taken?		
e)	Provide what temperature data is available by completing Table 3.		

2-12 Please identify person(s) to be contacted if clarification of the above information is necessary.

Name: ______________________ Phone No.: ____________

Name: ______________________ Phone No.: ____________

Mail to: Bob Howard (ECE MS 4-01)
(post office) Westinghouse Energy Center
P.O. Box 355
Pittsburgh, PA 15230-0355

COMPONENT RELIABILITY TEST DATA SHEET

(Fed Ex. to): 4350 Northern Pike
Monroeville, Pa., 15146

COMPONENT RELIABILITY TEST DATA SHEET

Section 3: Reactor Trip Breakers (RTBs)

Plant Name: ______________________________ Unit: ________

3-1 Please provide Reactor Trip Breaker maintenance history on this table. Breaker ID should consist of model and serial number. All changes to and repair of each RTB should be listed, including any breakers retired from service (give date of retirement). List any general refurbishments performed by the OEM. For example "Refurbished by Westinghouse NSD".

BREAKER ID	DATE	DESCRIPTION OF REPAIR OR REFURBISHMENT

COMPONENT RELIABILITY TEST DATA SHEET

3-2 List tests which impact the RTB or their appurtenances. The list should include all procedures which cause actuation of the components or collect data indicative of the component condition or environment. The test period should be on a per-component basis (enter "NO" if not periodic). Test Duration is the time the protection cabinet is out of service for the test. Describe the purpose/result of test (breaker trip, STA energizes, UVTA de-energizes).

No.	Procedure ID No.	Test Period	Test Duration	Description of test purpose/result

3-3	Routine Testing of Similar Equipment	YES	NO
a)	Are all components that perform the same function tested at the same period?		
b)	If "No", explain. Cite item number(s) from table above.		

COMPONENT RELIABILITY TEST DATA SHEET

3-4.	Routine maintenance/surveillance programs inspect for:	YES	NO
a)	Operation?		
b)	Condition of contacts?		
c)	Changes in appearance (color, texture)?		
d)	In-Cabinet "housekeeping"?		

3-5	Have "Failures" of the Reactor Trip Breakers been observed?	YES	NO
a)	During testing?		
b)	In-service under normal conditions?		
c)	In-service under abnormal conditions?		
d)	Complete Table 2, attached, listing all RTBs and their safety-related appurtenances (i.e., Shunt Trip Attachments and Undervoltage Trip Attachments).		

3-6	Cabinet Temperature Monitoring	YES	NO
a)	Is temperature monitored and controlled in the area of the Reactor Trip Switchgear cabinets (e.g., via Class 1E HVAC)?		
b)	If yes, what is the control setpoint for cooling?	°F	
c)	If yes to a) what is the control setpoint for heating?	°F	
d)	Describe the approximate location of temperature monitor relative to RTB cabinets:		

3-7	Cabinet Temperature Data:	YES	NO
a)	Are in-cabinet temperatures during normal operation known?		
b)	Are in-cabinet temperatures monitored routinely?		
c)	Were in-cabinet temperatures recorded on a one-time basis?		
d)	Have thermographic images of the cabinets been taken?		

COMPONENT RELIABILITY TEST DATA SHEET

e)	Provide what temperature data is available by completing Table 3.

3-8 Please identify person(s) to be contacted if clarification of the above information is necessary.

Name: ______________________________ Phone No.: ______________

Name: ______________________________ Phone No.: ______________

Mail to: Bob Howard (ECE MS 4-01)
(post office) Westinghouse Energy Center
P.O. Box 355
Pittsburgh, PA 15230-0355

(Fed Ex. to): 4350 Northern Pike
Monroeville, Pa., 15146

TABLE 1 EQUIPMENT/COMPONENT TEST PROCEDURES TABLE sheet ____ of ____

PLANT NAME & UNIT NO.: ____________________ PREPARED BY: ____________________

ITEM NO.	EQUIPMENT TESTED	TEST PERIOD	TEST DURATION	PLANT PROCEDURE NO.	DESCRIPTION OF TEST - PURPOSE OR OBJECTIVE

TABLE 2

COMPONENT RELIABILITY DATA TABLE

sheet ___ of ___

PLANT NAME & UNIT NO : ______________ SYSTEM. ______________ PREPARED BY: ______________

COMPON-ENT ID (1)	RELAY DATA:		INSTALLED/RE-PAIRED/ RE-PLACED (4)	TEST PERIOD (5)	TEST TYPE (6)	TOTAL ACTUA-TIONS (7)	FAILURES (8)	ROOT CAUSE (9)	NOTES (10)	REFS (11)
	TYPE (2)	COIL (3)								

Mail to: Bob Howard (ECE MS 4-01), P O. Box 355, Pittsburgh, PA 15230-0355 (post office), or Fed Ex address 4350 Northern Pike, Monroeville, Pa. 15146

• see attached instructions identifying desired information

INSTRUCTIONS FOR DATA TABLE

Data must be specific to each component, and each component should be identified by a model number or mnemonic (see instructions for Component ID (1)). Answer as completely as possible. Any data which is an estimate should be circled. If component replacements have occurred, such should be identified in Column (4); see instruction (4) below.
Questions or requests for clarification on the data sheet or table, please contact: R. C. (Bob) Howard 412-374-5217 or G. R. (Jerry) Andre 412-374-4723

(1) Component ID should refer to the system id number or mnemonics used in the applicable technical manuals. The ID should be descriptive of the component, its location and its function; SSPS relay K624-A. Relay Tag/ID numbers are provided in the SSPS tech manual or Relay Logic Schematic Drawings. Power supplies and circuit boards should be identified by their mnemonics or model (reference drawing) number, also found in schematic drawings and technical manuals For Reactor Trip Breakers, identify the model number (DB-50 or DS-416).

(2) This column applies to relays only. Enter: "BF", "BFD" or "NBFD" for Westinghouse BF type relays: "MG-6" for Westinghouse MG 6 relays, "CPC" for C.P Claire relays. MDX for Midtex relays. and KH for Potter & Brumfield KH relays) Any others, please specify. Use Notes, as necessary.

(3) This column applies to relays only. Please specify the relay coil type and state (during normal plant operation), as follows (e g., AC-NE = an AC coil relay normally energized during plant operation).

Enter' "AC" for AC current coils
"DC" for DC current coils

Enter: "ND" for normally de-energized coils
"NE" for normally energized
"NX" for normally de-energized; but energized during plant shutdown. (Please specify cumulative outage time relay energized in NOTES.

(4) Enter "X" for components that are original equipment. For components that replace OEM parts, enter date (month/year) on following line and respond in any columns that apply since the new relay was installed. State whether the relay or a part was repaired or replaced. Recall that the objective is to gather data after issuance of the plant operating license. Use Notes to provide details.

(5) For periodic operational tests, enter number of months between periodic tests (e g., "4"). Enter "R-xx" with xx= the nominal fuel cycle length, if component is tested only during plant/refueling outage. For other tests, enter N.A.

(6) Enter: "G" for "Go" testing; channel operates as normal and the "final device" is energized or operated (i e., RTB is tripped, pump is started)
Enter: "B" for "Block" testing, final device operation is prevented or simulated signal is used for detection only, no actuation occurs.
Enter: "OT" for periodic operational test, as for logic, master relay and RTBs
Enter: "PM" for post maintenance verification test.

(7) Total actuations is a count of mechanical cycle stress - this does not apply to circuit boards. The total actuations should include all experienced since issuance of operating license to date or until failure/replacement. This is to include any actuations which have involved other system tests which result in component actuations and any due to plant trips.

INSTRUCTIONS FOR DATA TABLE (cont)

(8) Failures should be characterized as one (or more) of the following:

"A" Did not actuate on demand.
"L" Did not latch when actuated.
"UL" Did not unlatch on demand.
"CO" Contact(s) did not make
"CI" Contact(s) or signal(s) exhibit intermittence.
"ERR" I&C circuit output other than expected; out of range or calibration
"ICO" General I&C circuit failure (open, short, grounded), failure is high or low, or not output produced.
"V" **Physical damage or significant degradation was observed visually. ("V" should be used in with other codes, and in all cases where it applies.)**
"N" None apply; add Notes (10) to describe.

(9) Root causes should be characterized as one of the following:

"U" if unknown or not determined.
"B" Binding of the relay (or other electromechanical device), "BD" if caused by dirt or debris,*
"O" Relay, STA or UVTA coil failed open or short.
"CA" Contact misalignment (relay or other electromechanical device)
"CW" Contact wear; note if corroded (CWC), pitted (CWP), or high resistance (CWR)*
"CF" Contacts fused or welded, "CFL" if due to excessive loading of contacts *
"LA" Latch misalignment in a relay or other electromechanical device
"LR" Latch reset coil open or shorted (relay or other electromechanical device)*
"S" Return spring broken or misaligned*
"O/S" Circuit open or short (PC board electronics)
"ICC" I&C channel calibration needed.
"FO-B" Failure within the RTB, not covered by the above; explain in Notes (10) column.
"V" **In addition to other symptoms, physical damage or significant degradation was observed visually. ("V" should be used in all cases where it applies.)**
"N" None apply; add Notes (10) to describe.

(10) Compile notes on separate sheet and attach. Make reference to all LERs or other documents which provide details.

(11) Enter applicable reference numbers. Compile list of references and attach.

TABLE 3 **TEMPERATURE DATA** sheet ____ of ____

PLANT NAME & UNIT NO.: ____________________ **PREPARED BY:** ____________________

SYSTEM	CABINET ID	Room Temp. Range		In-cabinet Temp. Range		How was temperature data gathered?
		Low	High	Low	High	