



OG-00-112  
November 8, 2000

WCAP-15376-P, Rev. 0  
WCAP-15377-NP, Rev. 0  
Project Number 694

**Domestic Members**

- AmerenUE
- Callaway
- American Electric Power Co.  
D.C. Cook 1 & 2
- Carolina Power & Light Co.  
H.B. Robinson 2  
Shearon Harris
- Commonwealth Edison  
Braidwood 1 & 2  
Byron 1 & 2
- Consolidated Edison  
Company of NY, Inc.  
Indian Point 2
- Duke Power Company  
Catawba 1 & 2  
McGuire 1 & 2
- First Energy Nuclear  
Operating Co.  
Beaver Valley 1 & 2
- Florida Power & Light Co.  
Turkey Point 3 & 4
- New York Power Authority  
Indian Point 3
- Northeast Utilities  
Seabrook  
Millstone 3
- Northern States Power Co.  
Prairie Island 1 & 2
- Pacific Gas & Electric Co.  
Diablo Canyon 1 & 2
- PSEG - Nuclear  
Salem 1 & 2
- Rochester Gas & Electric Co.  
R.E. Ginna
- South Carolina Electric  
& Gas Co.  
V.C. Summer
- STP Nuclear Operating Co.  
South Texas Project 1 & 2
- Southern Nuclear  
Operating Co.  
J.M. Farley 1 & 2  
A.W. Vogtle 1 & 2
- Tennessee Valley Authority  
Sequoyah 1 & 2  
Watts Bar 1
- TXU Electric  
Comanche Peak 1 & 2
- Virginia Power Co.  
North Anna 1 & 2  
Surry 1 & 2
- Wisconsin Electric Power Co.  
Point Beach 1 & 2
- Wisconsin Public Service Corp.  
Kewaunee
- Wolf Creek Nuclear  
Operating Corp.  
Wolf Creek

**International Members**

- Electrabel  
Doel 1, 2, 4  
Tihange 1, 3
- Kansai Electric Power Co.  
Mihama 1  
Takahama 1  
Ohi 1 & 2
- Korea Electric Power Co.  
Kori 1 - 4  
Yonggwang 1 & 2
- Nuclear Electric plc  
Sizewell B
- Nuklearna Elektrarna Krsko  
Krsko
- Spanish Utilities  
Asco 1 & 2  
Vandellios 2
- Almaraz 1 & 2
- Vattenfall AB  
Ringhals 2 - 4
- Taiwan Power Co.  
Maanshan 1 & 2

Document Control Desk  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555-0001

Attention: Chief, Information Management Branch,  
Division of Inspection and Support Programs

Subject: Westinghouse Owners Group  
Transmittal of Reports: WCAP-15376-P, Rev. 0, (Proprietary) and  
WCAP-15377-NP, Rev. 0, (Non-Proprietary), Entitled "Risk-  
Informed Assessment of the RTS and ESFAS Surveillance Test  
Intervals and Reactor Trip Breaker Test and Completion Times"  
(MUHP-3045)

This letter transmits fifteen (15) copies of the report WCAP-15376-P, Rev. 0, (Proprietary) and twelve (12) copies of the report WCAP-15377-NP, Rev. 0, (Non-Proprietary), both entitled "Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times," dated October 2000.

Also attached are:

1. One (1) copy of the Application of Withholding Proprietary Information from Public Disclosure, CAW-00-1429 (Non-Proprietary).
2. One (1) copy of Affidavit CAW-00-1429 (Non-Proprietary).
3. One (1) copy of the Copyright Notice.
4. One (1) copy of the Proprietary Information Notice.

WCAP-15376-P provides the technical justification for the following RTS Instrumentation (3.3.1), ESFAS Instrumentation (3.3.2), Containment Purge and Exhaust Isolation Instrumentation (3.3.6), CREFS Actuation Instrumentation (3.3.7), and BDPS (3.3.9) Technical Specification changes:

1. Relax the Reactor Trip Breaker Test Time from 2 hours to 4 hours,
2. Relax the Reactor Trip Breaker Completion Time from 1 hour to 24 hours,
3. Relax the Reactor Trip Breaker TRIP ACTUATING DEVICE OPERATIONAL TEST Surveillance Frequency from 2 months to 4 months,

*2048*  
*1/15 Prop Versions*  
*12 NP Versions*

OG-00-112  
November 8, 2000

4. Relax the Reactor Trip Breaker TRIP ACTUATING DEVICE OPERATIONAL TEST Surveillance Frequency from 2 months to 4 months,
5. Relax the RTS and ESFAS ACTUATION LOGIC TEST Surveillance Frequency from 2 months to 6 months,
6. Relax the RTS and ESFAS CHANNEL OPERATIONAL TEST Surveillance Frequency from 3 months to 6 months, and
7. Relax the ESFAS MASTER RELAY TEST Surveillance Frequency for SSPS plants from 2 months to 6 months.

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

The approach used in this program is consistent with Regulatory Guides 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 Decisionmaking: Technical Specifications." 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.

WCAP-15376-P, Rev. 0, provides the WOG technical documentation necessary to support licensees in amending their Technical Specifications. The WOG is submitting this licensing topical report, WCAP-15376-P, Rev. 0, under the NRC licensing topical report program for review and acceptance for referencing in licensing actions. The objective is that once approved, each WOG member may reference this report in amending their Technical Specifications.

The reports transmitted herewith each bear a Westinghouse copyright notice. The NRC is permitted to make the number of copies of the information contained in these reports which are necessary for its internal use in connection with generic and plant-specific reviews and approvals as well as the issuance, denial, amendment, transfer, renewal, modification, suspension, revocation, or violation of a license, permit, order, or regulation subject to the requirements of 10 CFR 2.790 regarding restrictions on public disclosure to the extent such information has been identified as proprietary by Westinghouse, copyright protection notwithstanding. With respect to the non-proprietary versions of these reports, the NRC is permitted to make the number of copies beyond those necessary for its internal use which are necessary in order to have one copy available for public viewing in the appropriate docket files in the public document room in Washington, DC and in local public document rooms as may be required by NRC regulations if the number of copies submitted is insufficient for this purpose. Copies made by the NRC must include the copyright notice in all instances and the proprietary notice if the original was identified as proprietary

As this report, WCAP-15376-P, Rev. 0, contains information proprietary to Westinghouse Electric Company, it is being transmitted with affidavits signed by Westinghouse, the owner of the information. The affidavits set forth the basis on which the information be withheld from public disclosure by the Commission and addresses with specificity the considerations listed in paragraph (b)(4) of Section 2.790 of the Commission's regulations. Accordingly, it is respectively requested that the information which is proprietary be withheld from public disclosure in accordance with 10CFR Section 2.790 of the Commission's regulations.

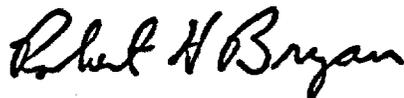
OG-00-112  
November 8, 2000

Correspondence with respect to the proprietary aspect of the Applications for Withholding or the supporting Westinghouse affidavits should reference CAW-00-1429 as appropriate and should be addressed to Mr. H.A. Sepp, Manager, Regulatory and Licensing Engineering, Westinghouse Electric Company, P. O. Box 355, Pittsburgh, PA 15230-0355. Invoices associated with the review of this WCAP should be addressed to:

Mr. Andrew P. Drake, Project Manager  
Westinghouse Owners Group  
Westinghouse Electric Company  
(Mail Stop ECE 5-16)  
P.O. Box 355  
Pittsburgh, PA 15230-0355

If you require further information, feel free to contact Mr. Ken Vavrek in the Westinghouse Owners Group Project Office at 412-374-4302.

Very truly yours,



Robert H. Bryan, Chairman  
Westinghouse Owners Group

attachments/ enclosures

cc: WOG Steering Committee (1L)  
WOG Primary Representatives (1L)  
WOG Licensing Subcommittee Representatives (1L)  
B. Barron, Duke Energy (1L)  
C. Bakken, AEP (1L)  
S. Bloom, USNRC (1L)  
R. Etling, W- ECE 5-43 (1L)  
H. A. Sepp, W- ECE 4-15 (1L)  
A. P. Drake, W- ECE 5-16 (1L)



Westinghouse Electric Company LLC

Box 355  
Pittsburgh Pennsylvania  
15230-0355

November 3, 2000

CAW-00-1429

Document Control Desk  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555

Attention: Mr. Samuel J. Collins

**APPLICATION FOR WITHHOLDING PROPRIETARY  
INFORMATION FROM PUBLIC DISCLOSURE**

**Subject: WCAP-15376-P, Rev. 0, "Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times," (Proprietary)**

Dear Mr. Collins:

The proprietary information for which withholding is being requested in the above-referenced report is further identified in Affidavit CAW-00-1429 signed by the owner of the proprietary information, Westinghouse Electric Company LLC. The affidavit, which accompanies this letter, sets forth the basis on which the information may be withheld from public disclosure by the Commission and addresses with specificity the considerations listed in paragraph (b)(4) of 10 CFR Section 2.790 of the Commission's regulations.

Accordingly, this letter authorizes the utilization of the accompanying Affidavit by the Westinghouse Owners Group.

Correspondence with respect to the proprietary aspects of the application for withholding or the Westinghouse affidavit should reference this letter, CAW-00-1429 and should be addressed to the undersigned.

Very truly yours,

H. A. Sepp, Manager  
Regulatory and Licensing Engineering

Enclosures

cc: T. Carter/NRC (5E7)

AFFIDAVIT

COMMONWEALTH OF PENNSYLVANIA:

SS

COUNTY OF ALLEGHENY:

Before me, the undersigned authority, personally appeared H. A. Sepp, who, being by me duly sworn according to law, deposes and says that he is authorized to execute this Affidavit on behalf of Westinghouse Electric Company LLC ("Westinghouse"), and that the averments of fact set forth in this Affidavit are true and correct to the best of his knowledge, information, and belief:



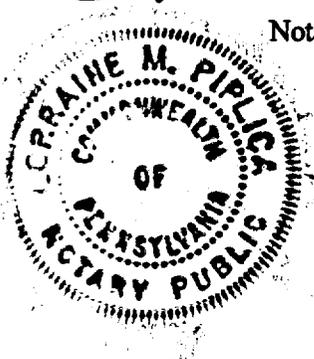
H. A. Sepp, Manager

Regulatory and Licensing Engineering

Sworn to and subscribed  
before me this 3<sup>RD</sup> day  
of November, 2000



Notary Public



Notarial Seal  
Lorraine M. Piplica, Notary Public  
Monroeville Boro, Allegheny County  
My Commission Expires Dec. 14, 2003  
Member, Pennsylvania Association of Notaries

- (1) I am Manager, Regulatory and Licensing Engineering, in the Nuclear Services Business Unit, of the Westinghouse Electric Company LLC ("Westinghouse"), and as such, I have been specifically delegated the function of reviewing the proprietary information sought to be withheld from public disclosure in connection with nuclear power plant licensing and rulemaking proceedings, and am authorized to apply for its withholding on behalf of the Westinghouse Electric Company LLC.
- (2) I am making this Affidavit in conformance with the provisions of 10CFR Section 2.790 of the Commission's regulations and in conjunction with the Westinghouse application for withholding accompanying this Affidavit.
- (3) I have personal knowledge of the criteria and procedures utilized by the Westinghouse Electric Company LLC in designating information as a trade secret, privileged or as confidential commercial or financial information.
- (4) Pursuant to the provisions of paragraph (b)(4) of Section 2.790 of the Commission's regulations, the following is furnished for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld.
  - (i) The information sought to be withheld from public disclosure is owned and has been held in confidence by Westinghouse.
  - (ii) The information is of a type customarily held in confidence by Westinghouse and not customarily disclosed to the public. Westinghouse has a rational basis for determining the types of information customarily held in confidence by it and, in that connection, utilizes a system to determine when and whether to hold certain types of information in confidence. The application of that system and the substance of that system constitutes Westinghouse policy and provides the rational basis required.

Under that system, information is held in confidence if it falls in one or more of several types, the release of which might result in the loss of an existing or potential competitive advantage, as follows:

- (a) The information reveals the distinguishing aspects of a process (or component, structure, tool, method, etc.) where prevention of its use by any of Westinghouse's competitors without license from Westinghouse constitutes a competitive economic advantage over other companies.
- (b) It consists of supporting data, including test data, relative to a process (or component, structure, tool, method, etc.), the application of which data secures a competitive economic advantage, e.g., by optimization or improved marketability.
- (c) Its use by a competitor would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing a similar product.
- (d) It reveals cost or price information, production capacities, budget levels, or commercial strategies of Westinghouse, its customers or suppliers.
- (e) It reveals aspects of past, present, or future Westinghouse or customer funded development plans and programs of potential commercial value to Westinghouse.
- (f) It contains patentable ideas, for which patent protection may be desirable.

There are sound policy reasons behind the Westinghouse system which include the following:

- (a) The use of such information by Westinghouse gives Westinghouse a competitive advantage over its competitors. It is, therefore, withheld from disclosure to protect the Westinghouse competitive position.
- (b) It is information which is marketable in many ways. The extent to which such information is available to competitors diminishes the Westinghouse ability to sell products and services involving the use of the information.

- (c) Use by our competitor would put Westinghouse at a competitive disadvantage by reducing his expenditure of resources at our expense.
  - (d) Each component of proprietary information pertinent to a particular competitive advantage is potentially as valuable as the total competitive advantage. If competitors acquire components of proprietary information, any one component may be the key to the entire puzzle, thereby depriving Westinghouse of a competitive advantage.
  - (e) Unrestricted disclosure would jeopardize the position of prominence of Westinghouse in the world market, and thereby give a market advantage to the competition of those countries.
  - (f) The Westinghouse capacity to invest corporate assets in research and development depends upon the success in obtaining and maintaining a competitive advantage.
- (iii) The information is being transmitted to the Commission in confidence and, under the provisions of 10CFR Section 2.790, it is to be received in confidence by the Commission.
- (iv) The information sought to be protected is not available in public sources or available information has not been previously employed in the same original manner or method to the best of our knowledge and belief.
- (v) The proprietary information sought to be withheld in this submittal is that which is appropriately marked in WCAP-15376-P, Rev. 0, "Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times," (Proprietary), October 2000 on behalf of the Westinghouse Owners Group by Westinghouse Electric Co., being transmitted by the Westinghouse Owners Group letter and Application for Withholding Proprietary Information from Public Disclosure, Mr. Robert H. Bryan, Chairman, Westinghouse Owners Group to the Document Control Desk, Attention Mr. Samuel J. Collins. The proprietary information as submitted for use by the Westinghouse Owners Group is applicable to other licensee submittals.

**This information is part of that which will enable Westinghouse to:**

- (a) Provide documentation of the fault trees used in the program to assess signal unavailabilites.**
- (b) Assist the customers in the licensing and NRC approval of the Technical Specification changes associated with this program.**

**Further this information has substantial commercial value as follows:**

- (a) Westinghouse can sell these fault trees in other analyses to support customer requests.**
- (b) Westinghouse can sell support and defense of the technology to its customers in the licensing process.**

**Public disclosure of this proprietary information is likely to cause substantial harm to the competitive position of Westinghouse because it would enhance the ability of competitors to provide similar calculation, evaluation and licensing defense services for commercial power reactors without commensurate expenses. Also, public disclosure of the information would enable others to use the information to meet NRC requirements for licensing documentation without purchasing the right to use the information.**

**The development of the technology described in part by the information is the result of applying the results of many years of experience in an intensive Westinghouse effort and the expenditure of a considerable sum of money.**

**In order for competitors of Westinghouse to duplicate this information, similar technical programs would have to be performed and a significant manpower effort, having the requisite talent and experience, would have to be expended for the development of analytical techniques and data in support of this program.**

**Further the deponent sayeth not.**

## **COPYRIGHT NOTICE**

The reports transmitted herewith each bear a Westinghouse copyright notice. The NRC is permitted to make the number of copies of the information contained in these reports which are necessary for its internal use in connection with generic and plant-specific reviews and approvals as well as the issuance, denial, amendment, transfer, renewal, modification, suspension, revocation, or violation of a license, permit, order, or regulation subject to the requirements of 10 CFR 2.790 regarding restrictions on public disclosure to the extent such information has been identified as proprietary by Westinghouse, copyright protection notwithstanding. With respect to the non-proprietary versions of these reports, the NRC is permitted to make the number of copies beyond those necessary for its internal use which are necessary in order to have one copy available for public viewing in the appropriate docket files in the public document room in Washington, DC and in local public document rooms as may be required by NRC regulations if the number of copies submitted is insufficient for this purpose. Copies made by the NRC must include the copyright notice in all instances and the proprietary notice if the original was identified as proprietary.

Westinghouse Non-Proprietary Class 3



WCAP - 15377

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

Westinghouse Electric Company LLC



WCAP-15377

Rev. 0

# **Risk-Informed Assessment of the RPS 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**

**October 2000**

This work was performed under WOG Shop Order MUHP-3045

---

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

©2000 Westinghouse Electric Company LLC  
All Rights Reserved

---

## LEGAL NOTICE

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

- (A) Makes any warranty or representation whatsoever, expressed 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
- (B) 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. Coding 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**

LIST OF TABLES.....	ix
LIST OF FIGURES.....	xi
ACRONYMS.....	xiii
ABSTRACT .....	xv
1.0 Introduction.....	1-1
2.0 Specific RTS, ESFAS, and Related Technical Specifications Evaluated .....	2-1
3.0 Need for Technical Specification STI and CT Changes .....	3-1
4.0 Technical Specification Change Request .....	4-1
5.0 NRC Meeting Summary .....	5-1
6.0 Design Basis Requirements and Impact .....	6-1
7.0 Reactor Protection System Description .....	7-1
7.1 RTS and ESFAS Design.....	7-1
7.2 Test and Maintenance Activities .....	7-4
8.0 Assessment of Impact On Risk .....	8-1
8.1 Tier 1: Approach to the Evaluation .....	8-2
8.1.1 Representative RPS Signals.....	8-2
8.1.2 Representative PRA Model .....	8-4
8.1.3 General Quantification Process .....	8-6
8.2 Data Development.....	8-9
8.2.1 Introduction.....	8-9
8.2.2 Components Included in Survey.....	8-10
8.2.3 Plant Survey .....	8-10
8.2.4 Calculation Methodology .....	8-14
8.2.5 Summary.....	8-14
8.3 RPS and ESFAS Signal Unavailability Analysis.....	8-16
8.3.1 Unavailability Analysis Approach.....	8-16
8.3.2 Assumptions.....	8-24
8.3.2.1 Analog Channels.....	8-24
8.3.2.2 Solid State Protection System.....	8-24
8.3.2.3 Relay Protection System .....	8-25
8.3.3 Fault Tree Models .....	8-26
8.3.4 Results of the Signal Unavailability Analysis.....	8-26
8.3.5 Comparison to WCAP-14333 and NUREG/CR-5500.....	8-47

---

---

**LIST OF TABLES**

Table 1.1	Summary of STI and CT Changes for the Various WOG Instrumentation Technical Specification Improvement Programs - Solid State Protection System (SSPS) .....	1-2
Table 1.2	Summary of STI and CT Changes for the Various WOG Instrumentation Technical Specification Improvement Programs - Relay Protection System .....	1-3
Table 4.1	Summary of RPS STI and CT Changes - Solid State Protection System .....	4-1
Table 4.2	Summary of RPS STI and CT Changes - Relay Protection System.....	4-1
Table 8.1	Summary of Signals Used in the Evaluation .....	8-3
Table 8.2	Solid State Protection System Master Relays.....	8-11
Table 8.3	Solid State Protection System Safeguards Driver Cards.....	8-12
Table 8.4	Relay Protection System Input Logic Relays .....	8-13
Table 8.5	Relay Protection System Master Relays .....	8-13
Table 8.6	Component Failure Probabilities.....	8-15
Table 8.7	Solid State Protection System Cases.....	8-20
Table 8.8	Relay Protection System Cases .....	8-22
Table 8.9	Summary of Safety Injection Unavailabilities: Solid State Protection System .....	8-31
Table 8.10	Summary of Auxiliary Feedwater Pump Start Signal Unavailabilities: Solid State Protection System.....	8-32
Table 8.11	Summary of Safety Injection and Auxiliary Feedwater Pump Start Signal Unavailabilities: Relay Protection System.....	8-33
Table 8.12	Summary of Reactor Trip Signal Unavailabilities: Solid State Protection System .....	8-34
Table 8.13	Summary of Reactor Trip Signal Unavailabilities: Relay Protection System....	8-35
Table 8.14	Breakdown of Signal Unavailability Contributors - SSPS Safety Injection: Pressurizer Pressure Low (2/4) Interlocked with P-11 .....	8-36

---

---

**LIST OF TABLES (cont.)**

Table 8.15	Breakdown of Signal Unavailability Contributors - SSPS Safety Injection: Pressurizer Pressure Low (2/4) Interlocked with P-11 with Operator Action .....	8-37
Table 8.16	Breakdown of Signal Unavailability Contributors - SSPS Auxiliary Feedwater Pump Start: Steam Generator Level Low-Low in One Loop (2/4) .....	8-38
Table 8.17	Breakdown of Signal Unavailability Contributors - SSPS Reactor Trip: Pressurizer Pressure High (2/4) .....	8-39
Table 8.18	Breakdown of Signal Unavailability Contributors - SSPS Reactor Trip: Pressurizer Pressure High (2/4) with Operator Action .....	8-40
Table 8.19	Breakdown of Signal Unavailability Contributors - SSPS Reactor Trip: Pressurizer Pressure High (2/3) or Overtemperature Delta T (2/4) .....	8-41
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 .....	8-42
Table 8.21	Dominant Cutsets for Signal Failure - Combined Case SSPS Safety Injection: Pressurizer Pressure Low (2/4) Interlocked with P-11 .....	8-43
Table 8.22	SSPS Auxiliary FW Pump Start: Steam Generator Level Low-Low in One Loop (2/4) .....	8-44
Table 8.23	Dominant Cutsets for Signal Failure - Combined Case SSPS Reactor Trip: Pressurizer Pressure High (2/4) .....	8-45
Table 8.24	Descriptions of Basic Event Identifiers Listed in Tables 8.21 to 8.23 .....	8-46
Table 8.25	Comparison of Signal Unavailabilities with Other Studies .....	8-47
Table 8.26	Sources of Reactor Trip Actuation Signals .....	8-50
Table 8.27	Sources of Engineered Safety Features Actuation Signals .....	8-51
Table 8.28	Summary of Human Error Probabilities for Operator Actions Backing Up Actuation Signals .....	8-52
Table 8.29	Summary of Results by Core Damage Frequency .....	8-55
Table 8.30	System (Top Event) Importance Summary: SSPS with 2 of 4 Logic .....	8-56
Table 8.31	System (Top Event) Importance Summary: SSPS with 2 of 3 Logic .....	8-57
Table 8.32	Summary of Results by Large Early Release Frequency .....	8-58
Table 8.33	Impact of Cumulative STI and CT Changes on Core Damage Frequency .....	8-59

---

**LIST OF FIGURES**

**Figure 7.1**    **Simplified Diagram of the Reactor Protection System.....7-3**

---

**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.

<b>Table 1.1 Summary of STI and AOT Changes for the Various WOG Instrumentation Technical Specification Improvement Programs (Solid State Protection System)</b>			
<b>Component</b>	<b>Pre-TOP</b>	<b>WCAP-10271 (TOP)</b>	<b>WCAP-14333</b>
<b>Analog Channels</b>			
- CT	1 hour	6 hours	72 hours
- Bypass Time	2 hours	4 hours	12 hours
- COT <sup>2</sup> STI	1 month	3 months	3 months
- Calibration Interval	NEAP <sup>1</sup>	NEAP <sup>1</sup>	18 months
- Calibration Time	NEAP <sup>1</sup>	NEAP <sup>1</sup>	4 hours
<b>Logic Cabinet</b>			
- CT	2 hours	6 hours	24 hours
- Bypass Time	1.5 hours	4 hours	4 hours
- STI	2 months	2 months	2 months
<b>Master Relay</b>			
- CT	2 hours	6 hours	24 hours
- Bypass Time	1.5 hours	4 hours	4 hours
- STI	2 months	2 months	2 months
<b>Slave Relay</b>			
- CT	2 hours	6 hours	24 hours
- Bypass Time	4 hours	4 hours	4 hours
- STI	3 months	3 months	3 months
<b>Reactor Trip Breakers</b>			
- 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 Operability Test (bypass or test time)

<b>Table 1.2 Summary of STI and AOT Changes for the Various WOG Instrumentation Technical Specification Improvement Programs (Relay Protection System)</b>			
<b>Component</b>	<b>Pre-TOP</b>	<b>WCAP-10271 (TOP)</b>	<b>WCAP-14333</b>
<b>Analog Channels</b>			
- CT	1 hour	6 hours	72 hours
- Bypass Time	2 hours	4 hours	12 hours
- COT <sup>2</sup> STI	1 month	3 months	3 months
- Calibration Interval	NEAP <sup>1</sup>	NEAP <sup>1</sup>	18 months
- Calibration Time	NEAP <sup>1</sup>	NEAP <sup>1</sup>	4 hours
<b>Logic Cabinet</b>			
- CT	2 hours	6 hours	24 hours
- Bypass Time	3 hours	8 hours	8 hours
- STI	1 month	1 month	1 month
<b>Master Relay</b>			
- CT	6 hours	6 hours	24 hours
- Bypass Time	3 hours	8 hours	8 hours
- STI	1 month	1 month	1 month
<b>Slave Relay</b>			
- CT	6 hours	6 hours	24 hours
- Bypass Time	6 hours	12 hours	12 hours
- STI	3 months	3 months	3 months
<b>Reactor Trip Breakers</b>			
- 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 Operability Test (bypass or test time)

## 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
	<u>OR</u> 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
	<u>OR</u> S.2 Be in MODE 3.	7 hours

(continued)

SURVEILLANCE REQUIREMENTS (continued)		
SURVEILLANCE		FREQUENCY
SR 3.3.1.4	<p>-----NOTE----- This Surveillance must be performed on the reactor trip bypass breaker prior to placing the bypass breaker in service. -----</p> <p>Perform TADOT.</p>	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	<p>-----NOTE----- Not required to be performed until [24] hours after THERMAL POWER is <math>\geq</math> 50% RTP. -----</p> <p>Calibrate excore channels to agree with incore detector measurements.</p>	[92] EFPD
SR 3.3.1.7	<p>-----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. -----</p> <p>Perform COT.</p>	[92] days

(continued)

ESFAS Instrumentation  
3.3.2

**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)

Containment Purge and Exhaust Isolation Instrumentation  
3.3.6

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

WOG STS

3.3-53

Rev 1, 04/07/95

CREFS Actuation Instrumentation  
3.3.7

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

WOG STS

3.3-58

Rev 1, 04/07/95

BDPS  
3.3.9

## ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
B. (continued)	B.2.2.2 Perform SR 3.1.1.1.	1 hour <u>AND</u> 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

WOG STS

3.3-65

Rev 1, 04/07/95

### 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 ability 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 6 hours 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.

<b>Component</b>	<b>Surveillance Test Intervals</b>	<b>Completion Times and Bypass Times</b>
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 <sup>1</sup>	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.

<b>Component</b>	<b>Surveillance Test Intervals</b>	<b>Completion Times and Bypass Times</b>
Logic Cabinet	1 month to 6 months	No changes
Master Relays	No change <sup>2</sup>	No changes
Analog Channels	3 months to 6 months	No changes
Reactor Trip Breakers	2 months to 4 months <sup>1</sup>	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 CCDF 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.

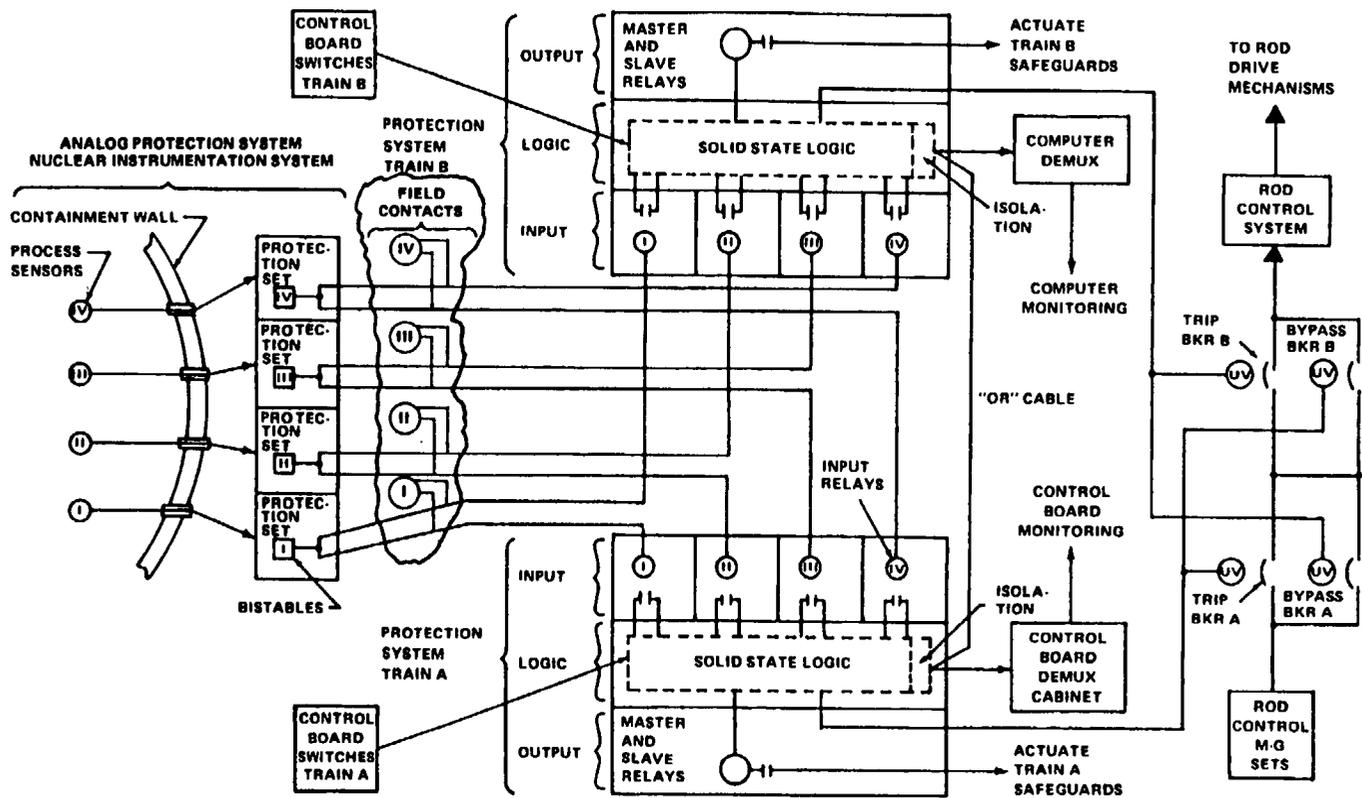


Figure 7.1 Simplified Diagram of the Reactor Protection System

## 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 provide 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.

<b>Table 8.1 Summary of Signals Used in the Evaluation</b>			
<b>Function</b>	<b>Logic Cabinet</b>	<b>Channel Logic</b>	<b>Operator Action</b>
SI <sup>1</sup>	SSPS	2 of 3	No
SI <sup>1</sup>	SSPS	2 of 4	No
SI <sup>1</sup>	SSPS	2 of 3	Yes
SI <sup>1</sup>	SSPS	2 of 4	Yes
SI <sup>1</sup>	Relay	2 of 3	No
SI <sup>1</sup>	Relay	2 of 4	No
AFWPS <sup>2</sup>	SSPS	2 of 3	No
AFWPS <sup>2</sup>	SSPS	2 of 4	No
AFWPS <sup>2</sup>	Relay	2 of 3	No
AFWPS <sup>2</sup>	Relay	2 of 4	No
RT <sup>3</sup>	SSPS	2 of 3	No
RT <sup>3</sup>	SSPS	2 of 4	No
RT <sup>4</sup>	SSPS	Diverse	No
RT <sup>3</sup>	SSPS	2 of 3	Yes
RT <sup>3</sup>	SSPS	2 of 4	Yes
RT <sup>4</sup>	SSPS	Diverse	Yes
RT <sup>3</sup>	Relay	2 of 3	No
RT <sup>3</sup>	Relay	2 of 4	No
RT <sup>4</sup>	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 signals to trip the reactor and initiate safety systems) is 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 injection. 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 isolation, 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 trip, and all the other events, except for large and medium type LOCAs, use a diverse signal.

---

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 in 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 cabinets 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 components 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          5.90E-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 in Section 8.2.3. The assumptions used for calculating the new reliability 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

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

- SSPS Safeguards Driver Cards
- Relay Protection System Input Logic Relays (Westinghouse BF and BFD input logic relays in relay protection system designs)
- Relay Protection 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 reliability was determined from the responses to this survey. A copy of the survey (Reference 11) is provided 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 participated in the survey. Column 2 of each table is the number of







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 calculating 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 reliability 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**

Table	Component	Failures/Demand

a,c

### 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 – [ ] <sup>a,c</sup>	Universal logic card – [ ] <sup>a,c</sup>
Master relays – [ ] <sup>a,c</sup>	Undervoltage driver card – [ ] <sup>a,c</sup>
Slave relays – [ ] <sup>a,c</sup>	Safeguards driver card – [ ] <sup>a,c</sup>
Power supplies – [ ] <sup>a,c</sup>	Test, blocking and RT contacts – [ ] <sup>a,c</sup>

(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:  $Q \times \beta \times \gamma \times (1-\delta)/3 \times \text{no. of common cause cutsets}$

Failure of 4 of 4 components:  $Q \times \beta \times \gamma \times \delta \times \text{no. of common cause cutsets}$

Failure of 2 of 3 components:  $Q \times \beta \times (1-\gamma)/2 \times \text{no. of common cause cutsets}$

Failure of 3 of 3 components:  $Q \times \beta \times \gamma \times \text{no. of common cause cutsets}$

where: Q - component failure probability

$\beta$  - Beta factor = [ ]<sup>a,c</sup>

$\gamma$  - Gamma factor = [ ]<sup>a,c</sup>

$\delta$  - Delta factor = [ ]<sup>a,c</sup>

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

$$= (4 \text{ hrs/test}) / (2 \text{ months/test} \times 730 \text{ hrs/month})$$

$$= 2.74\text{E-}03$$

where: test interval is 2 months

test time is 4 hours

Analog channel test and calibration unavailability

$$= (12 \text{ hrs/test}) / (3 \text{ months/test} \times 730 \text{ hrs/month}) +$$

$$((4 \text{ hrs/calibration}) / (18 \text{ months/calibration} \times 730 \text{ hrs/month}))$$

$$= 5.78\text{E-}03$$

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

$$= ((4 \text{ hrs/test}) / (2 \text{ months/test} \times 730 \text{ hrs/month})) +$$

$$((4 \text{ hrs/test}) / (2 \text{ months/test} \times 730 \text{ hrs/month}))$$

$$= 5.48\text{E-}03$$

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

$$= (2 \text{ hrs/test}) / (2 \text{ months/test} \times 730 \text{ hrs/month})$$

$$= 1.37\text{E-}03$$

---

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

Reactor trip breaker maintenance unavailability

$$= (6 \text{ hrs}/(1 \text{ yr} \times 8760 \text{ hrs/yr}))$$
$$= 6.85\text{E-}04$$

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:

$$FP = FR \times STI/2$$

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:

$$FP (\text{extended STI}) = FP (\text{current STI}) \times (\text{extended STI}/\text{current STI})$$

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

Parameter	Base Case	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6 <sup>1</sup>	Combined Case
<b>Analog Channels</b>								
- 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	<i>6 months</i>	3 months	3 months	3 months	3 months	3 months	<i>6 months</i>
- 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
<b>Logic Cabinet</b>								
- 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	<i>6 months</i>	2 months	2 months	2 months	2 months	<i>6 months</i>
<b>Master Relays</b>								
- 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	<i>6 months</i>	2 months	2 months	2 months	<i>6 months</i>

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

<b>Table 8.7 Solid State Protection System Cases (cont.)</b>								
<b>Parameter</b>	<b>Base Case</b>	<b>Case 1</b>	<b>Case 2</b>	<b>Case 3</b>	<b>Case 4</b>	<b>Case 5</b>	<b>Case 6</b>	<b>Combined Case</b>
<b>Slave Relays</b>								
- 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
<b>Reactor Trip Breakers</b>								
- Maint. Time	6 hours	6 hours	6 hours	6 hours	6 hours	<b>24+6 hours</b>	6 hours	<b>24+6 hours</b>
- 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	<b>4 hours</b>	2 hours	<b>4 hours</b>
- Test Interval	2 months	2 months	2 months	2 months	2 months	<b>6 months</b>	<b>4 months</b>	<b>4 months</b>

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

<b>Table 8.8 Relay Protection System Cases</b>							
<b>Parameter</b>	<b>Base Case</b>	<b>Case 1</b>	<b>Case 2</b>	<b>Case 3</b>	<b>Case 4</b>	<b>Case 5</b>	<b>Case 6</b>
<b>Analog Channels</b>							
- 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	<i>6 months</i>	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
<b>Logic Cabinet</b>							
- 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	<i>6 months</i>	N/A	1 month	1 month	1 month
<b>Master Relays</b>							
- 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.*

<b>Table 8.8 Relay Protection System Cases (cont.)</b>							
<b>Parameter</b>	<b>Base Case</b>	<b>Case 1</b>	<b>Case 2</b>	<b>Case 3</b>	<b>Case 4</b>	<b>Case 5</b>	<b>Case 6</b>
<b>Slave Relays</b>							
- 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
<b>Reactor Trip Breakers</b>							
- Maint. Time	6 hours	6 hours	6 hours	N/A	6 hours	<b>24+6 hours</b>	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	<b>4 hours</b>	2 hours
- Test Interval	2 months	2 months	2 months	N/A	<b>6 months</b>	2 months	<b>4 months</b>

*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 following 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 prohibit actuation of the entire associated train. This is consistent with actual practice and conservative.
3. Testing of the reactor trip breakers prohibits 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 prohibits 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 train. 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 practice.
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 following 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 logic.

2. The unavailabilities 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 with common cause failure contributions 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 primarily 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 than those for the SSPS. Based on this, it is concluded that the SSPS results are representative of the relay protection system results.

<b>Signal</b>	<b>Base Case</b>	<b>Case 1</b>	<b>Case 2</b>	<b>Case 3</b>	<b>Case 4</b>	<b>Case 5</b>	<b>Case 6</b>	<b>Combined Case</b>
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

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

<b>Signal</b>	<b>Base Case</b>	<b>Case 1</b>	<b>Case 2</b>	<b>Case 3</b>	<b>Case 4</b>	<b>Case 5</b>	<b>Case 6</b>
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

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

<b>Signal</b>	<b>Base Case</b>	<b>Case 1</b>	<b>Case 2</b>	<b>Case 3</b>	<b>Case 4</b>	<b>Case 5</b>	<b>Case 6</b>
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

Contributor	Unavailability Contributions			
	Base Case		Combined STIs and AOTs Case	
	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

Notes:

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

<b>Table 8.15 Breakdown of Signal Unavailability Contributors - SSPS Safety Injection: Pressurizer Pressure Low (2/4) Interlocked with P-11 with Operator Action</b>				
<b>Contributor</b>	<b>Unavailability Contributions</b>			
	<b>Base Case</b>		<b>Combined STIs and AOTs Case</b>	
	<b>Unavailability</b>	<b>Percent</b>	<b>Unavailability</b>	<b>Percent</b>
Random failures, test & maint.	8.52E-05	14.1	4.98E-05	8.6
<b>Common cause failures</b>				
- 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
<b>Total</b>	<b>6.05E-04</b>	<b>See Note 1</b>	<b>5.79E-04</b>	<b>See Note 1</b>

## Notes:

- 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)**

Contributor	Unavailability Contributions			
	Base Case		Combined STIs and AOTs Case	
	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

Notes:

- 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)**

Contributor	Unavailability Contributions			
	Base Case		Combined STIs and AOTs Case	
	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

Notes:

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

<b>Table 8.18 Breakdown of Signal Unavailability Contributors - SSPS Reactor Trip: Pressurizer Pressure High (2/4) with Operator Action</b>				
<b>Contributor</b>	<b>Unavailability Contributions</b>			
	<b>Base Case</b>		<b>Combined STIs and AOTs Case</b>	
	<b>Unavailability</b>	<b>Percent</b>	<b>Unavailability</b>	<b>Percent</b>
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

## Notes:

- 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)**

Contributor	Unavailability Contributions			
	Base Case		Combined STIs and AOTs Case	
	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

Notes:

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

<b>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</b>				
<b>Contributor</b>	<b>Unavailability Contributions</b>			
	<b>Base Case</b>		<b>Combined STIs and AOTs Case</b>	
	<b>Unavailability</b>	<b>Percent</b>	<b>Unavailability</b>	<b>Percent</b>
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

## Notes:

- 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 descriptions of basic event identifiers.

**Table 8.22 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.

<b>Signal</b>	<b>Current Study</b>	<b>WCAP-14333</b>	<b>NUREG/CR-5500</b>
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 importances based on contribution to core damage frequency. This importance function is defined as:

$$\text{Importance} = (\Sigma(\text{CDF of sequences with top event failure})/\text{total CDF}) \times 100$$

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.

<b>Event</b>	<b>Reactor Trip Actuation Signal</b>	<b>Operation Action</b>
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

<b>Safety Function</b>	<b>Event</b>	<b>Signal Actuation Source</b>
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

<b>Operator Action</b>	<b>HEP (1)</b>	<b>Source</b>
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:

$$\text{ICCDP} = [(\text{conditional CDF with subject equipment out of service}) - (\text{baseline CDF with nominal expected equipment unavailabilities})] \times (\text{duration of single AOT under consideration}) \quad (\text{Reference 2})$$

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-04 per year from Table 8.29. Two CTs are considered; 30 hours for maintenance and 4 hours for a test. The above equation becomes:

$$\begin{aligned} \text{ICCDP} &= (7.07\text{E-}05/\text{yr} - 5.05\text{E-}05/\text{yr}) \times 30 \text{ hrs}/(8760 \text{ hrs}/\text{yr}) = 6.92\text{E-}08, \text{ and} \\ \text{ICCDP} &= (7.07\text{E-}05/\text{yr} - 5.05\text{E-}05/\text{yr}) \times 4 \text{ hrs}/(8760 \text{ hrs}/\text{yr}) = 9.22\text{E-}09 \end{aligned}$$

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.

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

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%

System	Importance Measure	
	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 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%

Case	Parameter Change	2/4 Logic			2/3 Logic		
		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.

<b>Case</b>	<b>2/4 Logic</b>	<b>2/3 Logic</b>
CDF Impact: Pre-TOP to WCAP-14333	-2.3E-07/yr	2.4E-07/yr
CDF Impact: WCAP-14333 to Current Request	8.03E-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:

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

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 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 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 simultaneously.

- 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, "Surry 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 Energy Systems  
Electric Corporation

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: Mr. R.C. Howard (ECE MS 4-01)  
Westinghouse Electric Corporation  
P.O. Box 355  
Pittsburgh, PA 15230-0355

Fax to: (412) 374-5099

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,

  
H.A. Sepp  
Interim Project Manager  
Westinghouse Owners Group

JDC/HAS/ygs  
attachment

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

L3045SUR.wpd

---

**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	Replaced in kind?	If not replaced in kind, replacement type is:
			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	

- 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**

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





### 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	Enter: "ND" for normally de-energized coils
"DC" for DC current 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.



**APPENDIX B**  
**MARKED-UP TECHNICAL SPECIFICATIONS AND BASES**

## ACTIONS (continued)

CONDITION	REQUIRED ACTION	COMPLETION TIME
R. One RTB train inoperable.	-----NOTES----- 1. One train may be bypassed for up to <del>2</del> <sup>4</sup> hours for surveillance testing, provided the other train is OPERABLE.	
	<del>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.</del>	
	R.1 Restore train to OPERABLE status.	24 hours
	<u>OR</u> R.2 Be in MODE 3.	30 hours
S. One channel inoperable.	S.1 Verify interlock is in required state for existing unit conditions.	1 hour
	<u>OR</u> S.2 Be in MODE 3.	7 hours

(continued)

RTS Instrumentation  
3.3.1

## 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.	62 21 days on a STAGGERED TEST BASIS
SR 3.3.1.5 Perform ACTUATION LOGIC TEST.	92 21 days on a STAGGERED TEST BASIS
SR 3.3.1.6 -----NOTE----- Not required to be performed until [24] hours after THERMAL POWER is $\geq$ 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.	184 [92] days

(continued)

**BASES****ACTIONS**Q.1 and Q.2 (continued)

next 6 hours. The Completion Time of 6 hours (Required Action Q.1) is reasonable considering that in this Condition, the remaining OPERABLE train is adequate to perform the safety function and given the low probability of an event during this interval. The Completion Time of 6 hours (Required Action Q.2) is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging unit systems.

The Required Actions have been modified by a Note that allows bypassing one train up to [4] hours for surveillance testing, provided the other train is OPERABLE.

R.1 and R.2

Condition R applies to the RTBs in MODES 1 and 2. These actions address the train orientation of the RTS for the RTBs. ~~With one train inoperable, 1 hour is allowed to restore the train to OPERABLE status or the unit must be placed in MODE 3 within the next 6 hours. The Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging unit systems. The 1 hour and 6 hour Completion Times are equal to the time allowed by LCD 3.0.3 for shutdown actions in the event of a complete loss of RTS Function. Placing the unit in MODE 3 removes the requirement for this particular Function.~~

The Required Actions have been modified by ~~two~~ <sup>two</sup> Notes. ~~Note 1 allows one channel to be bypassed for up to 2 hours for surveillance testing, provided the other channel is OPERABLE. Note 2 allows one RTB to be bypassed for up to 2 hours for maintenance on undervoltage of shunt trip mechanisms if the other RTB train is OPERABLE. The 2 hour time limit is justified in Reference 1.~~

S.1 and S.2

Condition S applies to the P-6 and P-10 interlocks. With one channel inoperable for one-out-of-two or two-out-of-four coincidence logic, the associated interlock must be verified to be in its required state for the existing unit condition

(continued)

**Insert 1**

**The 24 hour Completion Time is justified in Reference 9.**

## BASES

SURVEILLANCE  
REQUIREMENTS  
(continued)SR 3.3.1.4

62

SR 3.3.1.4 is the performance of a TADOT every ~~31~~ days on a STAGGERED TEST BASIS. This test shall verify OPERABILITY by actuation of the end devices.

The RTB test shall include separate verification of the undervoltage and shunt trip mechanisms. Independent verification of RTB undervoltage and shunt trip Function is not required for the bypass breakers. No capability is provided for performing such a test at power. The independent test for bypass breakers is included in SR 3.3.1.14. The bypass breaker test shall include a local shunt trip. A Note has been added to indicate that this test must be performed on the bypass breaker prior to placing it in service.

62

*justified in  
Reference 9.*

The Frequency of every ~~31~~ days on a STAGGERED TEST BASIS is adequate. It is based on industry operating experience ~~considering instrument reliability and operating history data.~~

SR 3.3.1.5

92

SR 3.3.1.5 is the performance of an ACTUATION LOGIC TEST. The SSPS is tested every ~~31~~ days on a STAGGERED TEST BASIS, using the semiautomatic tester. The train being tested is placed in the bypass condition, thus preventing inadvertent actuation. Through the semiautomatic tester, all possible logic combinations, with and without applicable permissives, are tested for each protection function. The Frequency of every ~~31~~ days on a STAGGERED TEST BASIS is adequate. It is based on industry operating experience, considering instrument reliability and operating history data.

92

*justified in Reference 9.*

SR 3.3.1.6

SR 3.3.1.6 is a calibration of the excore channels to the incore channels. If the measurements do not agree, the excore channels are not declared inoperable but must be calibrated to agree with the incore detector measurements. If the excore channels cannot be adjusted, the channels are declared inoperable. This Surveillance is performed to verify the f( $\Delta I$ ) input to the overtemperature  $\Delta T$  Function.

(continued)

## BASES

SURVEILLANCE  
REQUIREMENTSSR 3.3.1.6 (continued)

A Note modifies SR 3.3.1.6. The Note states that this Surveillance is required only if reactor power is > 50% RTP and that [24] hours is allowed for performing the first surveillance after reaching 50% RTP.

The Frequency of 92 EFPD is adequate. It is based on industry operating experience, considering instrument reliability and operating history data for instrument drift.

SR 3.3.1.7

SR 3.3.1.7 is the performance of a COT every [92] days. 184

A COT is performed on each required channel to ensure the entire channel will perform the intended Function.

Setpoints must be within the Allowable Values specified in Table 3.3.1-1.

The difference between the current "as found" values and the previous test "as left" values must be consistent with the drift allowance used in the setpoint methodology. The setpoint shall be left set consistent with the assumptions of the current unit specific setpoint methodology.

The "as found" and "as left" values must also be recorded and reviewed for consistency with the assumptions of Reference ~~7~~.  
6

SR 3.3.1.7 is modified by a Note that provides a 4 hour delay in the requirement to perform this Surveillance for source range instrumentation when entering MODE 3 from MODE 2. This Note allows a normal shutdown to proceed without a delay for testing in MODE 2 and for a short time in MODE 3 until the RTBs are open and SR 3.3.1.7 is no longer required to be performed. If the unit is to be in MODE 3 with the RTBs closed for > 4 hours this Surveillance must be performed prior to 4 hours after entry into MODE 3.

The Frequency of [92] days is justified in Reference ~~7~~.  
184 9

(continued)

**BASES**

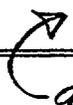
---

**REFERENCES**

(continued)

5. 10 CFR 50.49.
6. RTS/ESFAS Setpoint Methodology Study.
7. WCAP-10271-P-A, Supplement 2, Rev. 1, June 1990.
8. Technical Requirements Manual, Section 15, "Response Times."

---



9. WCAP-15376, Rev. 0, October 2000.

ESFAS Instrumentation  
3.3.2

## 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.	<del>31</del> <sup>92</sup> 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.	<del>31</del> <sup>92</sup> days on a STAGGERED TEST BASIS(4)
SR 3.3.2.5 Perform COT.	<del>92</del> <sup>124</sup> days
SR 3.3.2.6 Perform SLAVE RELAY TEST.	[92] days

(continued)

*Insert 2*

Insert 2

- (a) Reviewer's Note: The Frequency remains at 31 days on a STAGGERED TEST BASIS for plants with a Relay Protection System.

ESFAS Instrumentation  
B 3.3.2

## BASES

## ACTIONS

SR 3.3.2.1 (continued)

approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the unit staff, based on a combination of the channel instrument uncertainties, including indication and reliability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit.

The Frequency is based on operating experience that demonstrates channel failure is rare. The CHANNEL CHECK supplements less formal, but more frequent, checks of channels during normal operational use of the displays associated with the LCO required channels.

SR 3.3.2.2

92 SR 3.3.2.2 is the performance of an ACTUATION LOGIC TEST. The SSPS is tested every 31 days on a STAGGERED TEST BASIS, using the semiautomatic tester. The train being tested is placed in the bypass condition, thus preventing inadvertent actuation. Through the semiautomatic tester, all possible logic combinations, with and without applicable permissives, are tested for each protection function. In addition, the master relay coil is pulse tested for continuity. This verifies that the logic modules are OPERABLE and that there is an intact voltage signal path to the master relay coils. 92 The Frequency of every 31 days on a STAGGERED TEST BASIS is adequate. It is based on industry operating experience, considering instrument reliability and operating history data. justified in Reference 10.

SR 3.3.2.3

SR 3.3.2.3 is the performance of an ACTUATION LOGIC TEST as described in SR 3.3.2.2, except that the semiautomatic

(continued)

BASESSURVEILLANCE  
REQUIREMENTSSR 3.3.2.3 (continued)

tester is not used and the continuity check does not have to be performed, as explained in the Note. This SR is applied to the balance of plant actuation logic and relays that do not have the SSPS test circuits installed to utilize the semiautomatic tester or perform the continuity check. This test is also performed every 31 days on a STAGGERED TEST BASIS. The Frequency is adequate based on industry operating experience, considering instrument reliability and operating history data.

SR 3.3.2.4

SR 3.3.2.4 is the performance of a MASTER RELAY TEST. The MASTER RELAY TEST is the energizing of the master relay, verifying contact operation and a low voltage continuity check of the slave relay coil. Upon master relay contact operation, a low voltage is injected to the slave relay coil. This voltage is insufficient to pick up the slave relay, but large enough to demonstrate signal path continuity. This test is performed every ~~31~~ <sup>92</sup> days on a STAGGERED TEST BASIS. The time allowed for the testing (4 hours) and the surveillance interval are justified in Reference 8. *Insert 3* <sup>1/5</sup>

SR 3.3.2.5

SR 3.3.2.5 is the performance of a COT.

A COT is performed on each required channel to ensure the entire channel will perform the intended Function. Setpoints must be found within the Allowable Values specified in Table 3.3.1-1.

The difference between the current "as found" values and the previous test "as left" values must be consistent with the drift allowance used in the setpoint methodology. The setpoint shall be left set consistent with the assumptions of the current unit specific setpoint methodology.

The "as found" and "as left" values must also be recorded and reviewed for consistency with the assumptions of the *Reference 6.*

(continued)

Insert 3

The Frequency of [92] days is justified in Reference 10.

## BASES

SURVEILLANCE  
REQUIREMENTSSR 3.3.2.5 (continued)

~~surveillance interval extension analysis (Ref. 8) when applicable.~~

The Frequency of ~~92~~ days is justified in Reference ~~8~~.  
184 10

SR 3.3.2.6

SR 3.3.2.6 is the performance of a SLAVE RELAY TEST. The SLAVE RELAY TEST is the energizing of the slave relays. Contact operation is verified in one of two ways. Actuation equipment that may be operated in the design mitigation MODE is either allowed to function, or is placed in a condition where the relay contact operation can be verified without operation of the equipment. Actuation equipment that may not be operated in the design mitigation MODE is prevented from operation by the SLAVE RELAY TEST circuit. For this latter case, contact operation is verified by a continuity check of the circuit containing the slave relay. This test is performed every [92] days. The Frequency is adequate, based on industry operating experience, considering instrument reliability and operating history data.

SR 3.3.2.7

SR 3.3.2.7 is the performance of a TADOT every [92] days. This test is a check of the Loss of Offsite Power, Undervoltage RCP, and AFW Pump Suction Transfer on Suction Pressure—Low Functions. Each Function is tested up to, and including, the master transfer relay coils.

The test also includes trip devices that provide actuation signals directly to the SSPS. The SR is modified by a Note that excludes verification of setpoints for relays. Relay setpoints require elaborate bench calibration and are verified during CHANNEL CALIBRATION. The Frequency is adequate. It is based on industry operating experience, considering instrument reliability and operating history data.

(continued)

ESFAS Instrumentation  
B 3.3.2

---

BASESSURVEILLANCE  
REQUIREMENTSSR 3.3.2.11 (continued)

Trip Interlock, and the Frequency is once per RTB cycle. This Frequency is based on operating experience demonstrating that undetected failure of the P-4 interlock sometimes occurs when the RTB is cycled.

The SR is modified by a Note that excludes verification of setpoints during the TADOT. The Function tested has no associated setpoint.

---

REFERENCES

1. FSAR, Chapter [6].
2. FSAR, Chapter [7].
3. FSAR, Chapter [15].
4. IEEE-279-1971.
5. 10 CFR 50.49.
6. RTS/ESFAS Setpoint Methodology Study.
7. NUREG-1218, April 1988.
8. WCAP-10271-P-A, Supplement 2, Rev. 1, June 1990.
9. Technical Requirements Manual, Section 15, "Response Times."

---

10. WCAP-15376, Rev. 0, October 2000.

WOG STS

B 3.3-120

Rev 1, 04/07/95

Containment Purge and Exhaust Isolation Instrumentation  
3.3.6

## 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
<i>Insert 4</i> SR 3.3.6. <sup>6</sup> Perform COT.	92 days
SR 3.3.6. <sup>7</sup> Perform SLAVE RELAY TEST.	[92] days
SR 3.3.6. <sup>8</sup> -----NOTE----- Verification of setpoint is not required. ----- Perform TADOT.	[18] months
SR 3.3.6. <sup>9</sup> Perform CHANNEL CALIBRATION.	[18] months

*Insert 8*

WOG STS

3.3-53

Rev 1, 04/07/95

## Insert 4

---

NOTE

---

This Surveillance is only applicable to the actuation logic of the ESFAS Instrumentation.

---

SR	3.3.6.4	Perform ACTUATION LOGIC TEST.	92 days on a STAGGERED TEST BASIS <sup>(a)</sup>
----	---------	-------------------------------	--

---

---

NOTE

---

This Surveillance is only applicable to the master relays of the ESFAS Instrumentation.

---

SR	3.3.6.5	Perform MASTER RELAY TEST.	92 days on a STAGGERED TEST BASIS <sup>(b)</sup>
----	---------	----------------------------	--

Insert 8

- (a) Reviewer's Note: The Frequency of 92 days on a STAGGERED TEST BASIS is applicable to the actuation logic processed through the Relay or Solid State Protection System.
- (b) Reviewer's Note: The Frequency of 92 days on a STAGGERED TEST BASIS is applicable to the master relays processed through the Solid State Protection System.

Containment Purge and Exhaust Isolation Instrumentation  
B 3.3.6

**BASES**

---

**SURVEILLANCE  
REQUIREMENTS**

SR 3.3.6.1 (continued)

channels during normal operational use of the displays associated with the LCO required channels.

SR 3.3.6.2

SR 3.3.6.2 is the performance of an ACTUATION LOGIC TEST. The train being tested is placed in the bypass condition, thus preventing inadvertent actuation. Through the semiautomatic tester, all possible logic combinations, with and without applicable permissives, are tested for each protection function. In addition, the master relay coil is pulse tested for continuity. This verifies that the logic modules are OPERABLE and there is an intact voltage signal path to the master relay coils. This test is performed every 31 days on a STAGGERED TEST BASIS. The Surveillance interval is acceptable based on instrument reliability and industry operating experience.

SR 3.3.6.3

SR 3.3.6.3 is the performance of a MASTER RELAY TEST. The MASTER RELAY TEST is the energizing of the master relay, verifying contact operation and a low voltage continuity check of the slave relay coil. Upon master relay contact operation, a low voltage is injected to the slave relay coil. This voltage is insufficient to pick up the slave relay, but large enough to demonstrate signal path continuity. This test is performed every 31 days on a STAGGERED TEST BASIS. The Surveillance interval is acceptable based on instrument reliability and industry operating experience.

*Insert 5 →*

SR 3.3.6.4

A COT is performed every 92 days on each required channel to ensure the entire channel will perform the intended function. The frequency is based on the staff recommendation for increasing the availability of radiation monitors according to NUREG-1366 (Ref. 2). This test verifies the capability of the instrumentation to provide the containment purge and exhaust system isolation. The

(continued)

WOG STS

B 3.3-156

Rev 1, 04/07/95

## Insert 5

SR 3.3.6.4

SR 3.3.6.4 is the performance of an ACTUATION LOGIC TEST. The train being tested is placed in the bypass condition, thus preventing inadvertent actuation. Through the semiautomatic tester, all possible logic combinations, with and without applicable permissives, are tested for each protection function. In addition, the master relay coil is pulse tested for continuity. This verifies that the logic modules are OPERABLE and there is an intact voltage signal path to the master relay coils. This test is performed every 92 days on a STAGGERED TEST BASIS. The Surveillance interval is justified in Reference 3.

The SR is modified by a Note stating that the Surveillance is only applicable to the actuation logic of the ESFAS Instrumentation.

SR 3.3.6.5

SR 3.3.6.5 is the performance of a MASTER RELAY TEST. The MASTER RELAY TEST is the energizing of the master relay, verifying contact operation and a low voltage continuity check of the slave relay coil. Upon master relay contact operation, a low voltage is injected to the slave relay coil. This voltage is insufficient to pick up the slave relay, but large enough to demonstrate signal path continuity. This test is performed every 92 days on a STAGGERED TEST BASIS. The Surveillance interval is justified in Reference 3.

The SR is modified by a Note stating that the Surveillance is only applicable to the master relays of the ESFAS Instrumentation.

Containment Purge and Exhaust Isolation Instrumentation  
B 3.3.6

BASES

---

SURVEILLANCE  
REQUIREMENTS

SR 3.3.6.<sup>6</sup> (continued)

setpoint shall be left consistent with the current unit specific calibration procedure tolerance.

SR 3.3.6.<sup>7</sup>

SR 3.3.6.5 is the performance of a SLAVE RELAY TEST. The SLAVE RELAY TEST is the energizing of the slave relays. Contact operation is verified in one of two ways. Actuation equipment that may be operated in the design mitigation mode is either allowed to function or is placed in a condition where the relay contact operation can be verified without operation of the equipment. Actuation equipment that may not be operated in the design mitigation mode is prevented from operation by the SLAVE RELAY TEST circuit. For this latter case, contact operation is verified by a continuity check of the circuit containing the slave relay. This test is performed every [92] days. The Frequency is acceptable based on instrument reliability and industry operating experience.

SR 3.3.6.<sup>8</sup>

SR 3.3.6.6 is the performance of a TADOT. This test is a check of the Manual Actuation Functions and is performed every [18] months. Each Manual Actuation Function is tested up to, and including, the master relay coils. In some instances, the test includes actuation of the end device (i.e., pump starts, valve cycles, etc.).

The test also includes trip devices that provide actuation signals directly to the SSPS, bypassing the analog process control equipment. The SR is modified by a Note that excludes verification of setpoints during the TADOT. The Functions tested have no setpoints associated with them.

The Frequency is based on the known reliability of the Function and the redundancy available, and has been shown to be acceptable through operating experience.

(continued)

Containment Purge and Exhaust Isolation Instrumentation  
B 3.3.6

---

**BASES**

**SURVEILLANCE  
REQUIREMENTS**  
(continued)

<sup>9</sup>  
SR 3.3.6.7

A CHANNEL CALIBRATION is performed every [18] months, or approximately at every refueling. CHANNEL CALIBRATION is a complete check of the instrument loop, including the sensor. The test verifies that the channel responds to a measured parameter within the necessary range and accuracy.

The Frequency is based on operating experience and is consistent with the typical industry refueling cycle.

---

**REFERENCES**

1. 10 CFR 100.11.
2. NUREG-1366, [date].

---

3. WCAP-15376, Rev. 0, October 2000.

CREFS Actuation Instrumentation  
3.3.7

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
<i>Insert 6 →</i> SR 3.3.7. <sup>7</sup> <del>8</del> Perform SLAVE RELAY TEST.	[92] days
SR 3.3.7. <sup>8</sup> <del>9</del> -----NOTE----- Verification of setpoint is not required. ----- Perform TADOT.	[18] months
SR 3.3.7. <sup>9</sup> <del>8</del> Perform CHANNEL CALIBRATION.	[18] months

*Insert 8*

WOG STS

3.3-58

Rev 1, 04/07/95

## Insert 6

---

~~NOTE~~

---

This Surveillance is only applicable to the actuation logic of the ESFAS Instrumentation.

---

SR	3.3.7.5	Perform ACTUATION LOGIC TEST.	92 days on a STAGGERED TEST BASIS <sup>(a)</sup>
----	---------	-------------------------------	--

---

---

~~NOTE~~

---

This Surveillance is only applicable to the master relays of the ESFAS Instrumentation.

---

SR	3.3.7.6	Perform MASTER RELAY TEST.	92 days on a STAGGERED TEST BASIS <sup>(b)</sup>
----	---------	----------------------------	--

## Insert 8

- (a) Reviewer's Note: The Frequency of 92 days on a STAGGERED TEST BASIS is applicable to the actuation logic processed through the Relay or Solid State Protection System.
- (b) Reviewer's Note: The Frequency of 92 days on a STAGGERED TEST BASIS is applicable to the master relays processed through the Solid State Protection System.

BASESSURVEILLANCE  
REQUIREMENTSSR 3.3.7.1 (continued)

including indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit.

The Frequency is based on operating experience that demonstrates channel failure is rare. The CHANNEL CHECK supplements less formal, but more frequent, checks of channels during normal operational use of the displays associated with the LCO required channels.

SR 3.3.7.2

A COT is performed once every 92 days on each required channel to ensure the entire channel will perform the intended function. This test verifies the capability of the instrumentation to provide the CREFS actuation. The setpoints shall be left consistent with the unit specific calibration procedure tolerance. The Frequency is based on the known reliability of the monitoring equipment and has been shown to be acceptable through operating experience.

SR 3.3.7.3

SR 3.3.7.3 is the performance of an ACTUATION LOGIC TEST. The train being tested is placed in the bypass condition, thus preventing inadvertent actuation. Through the semiautomatic tester, all possible logic combinations, with and without applicable permissives, are tested for each protection function. In addition, the master relay coil is pulse tested for continuity. This verifies that the logic modules are OPERABLE and there is an intact voltage signal path to the master relay coils. This test is performed every 31 days on a STAGGERED TEST BASIS. The Frequency is justified in WCAP-10271-P-A, Supplement 2, Rev 1 (Ref 1).

*acceptable based on instruments reliability and industry operating experience.*

SR 3.3.7.4

SR 3.3.7.4 is the performance of a MASTER RELAY TEST. The MASTER RELAY TEST is the energizing of the master relay, verifying contact operation and a low voltage continuity

(continued)

CREFS Actuation Instrumentation  
B 3.3.7

BASES

SURVEILLANCE  
REQUIREMENTS

SR 3.3.7.4 (continued)

check of the slave relay coil. Upon master relay contact operation, a low voltage is injected to the slave relay coil. This voltage is insufficient to pick up the slave relay, but large enough to demonstrate signal path continuity. This test is performed every 31 days on a STAGGERED TEST BASIS. The Frequency is acceptable based on instrument reliability and industry operating experience.

*Intent 7 → 7*  
SR 3.3.7.5

SR 3.3.7.5 is the performance of a SLAVE RELAY TEST. The SLAVE RELAY TEST is the energizing of the slave relays. Contact operation is verified in one of two ways. Actuation equipment that may be operated in the design mitigation MODE is either allowed to function or is placed in a condition where the relay contact operation can be verified without operation of the equipment. Actuation equipment that may not be operated in the design mitigation MODE is prevented from operation by the SLAVE RELAY TEST circuit. For this latter case, contact operation is verified by a continuity check of the circuit containing the slave relay. This test is performed every [92] days. The Frequency is acceptable based on instrument reliability and industry operating experience.

SR 3.3.7.6

SR 3.3.7.6 is the performance of a TADOT. This test is a check of the Manual Actuation Functions and is performed every [18] months. Each Manual Actuation Function is tested up to, and including, the master relay coils. In some instances, the test includes actuation of the end device (i.e., pump starts, valve cycles, etc.).

The test also includes trip devices that provide actuation signals directly to the Solid State Protection System, bypassing the analog process control equipment. The Frequency is based on the known reliability of the Function and the redundancy available, and has been shown to be acceptable through operating experience. The SR is modified by a Note that excludes verification of setpoints during the

(continued)

## Insert 7

SR 3.3.7.5

SR 3.3.7.5 is the performance of an ACTUATION LOGIC TEST. The train being tested is placed in the bypass condition, thus preventing inadvertent actuation. Through the semiautomatic tester, all possible logic combinations, with and without applicable permissives, are tested for each protection function. In addition, the master relay coil is pulse tested for continuity. This verifies that the logic modules are OPERABLE and there is an intact voltage signal path to the master relay coils. This test is performed every 92 days on a STAGGERED TEST BASIS. The Surveillance interval is justified in Reference 1.

The SR is modified by a Note stating that the Surveillance is only applicable to the actuation logic of the ESFAS Instrumentation.

SR 3.3.7.6

SR 3.3.7.6 is the performance of a MASTER RELAY TEST. The MASTER RELAY TEST is the energizing of the master relay, verifying contact operation and a low voltage continuity check of the slave relay coil. Upon master relay contact operation, a low voltage is injected to the slave relay coil. This voltage is insufficient to pick up the slave relay, but large enough to demonstrate signal path continuity. This test is performed every 92 days on a STAGGERED TEST BASIS. The Surveillance interval is justified in Reference 1.

The SR is modified by a Note stating that the Surveillance is only applicable to the master relays of the ESFAS Instrumentation.

CREFS Actuation Instrumentation  
B 3.3.7

---

BASESSURVEILLANCE  
REQUIREMENTSSR 3.3.7.<sup>8</sup> (continued)

TADOT. The Functions tested have no setpoints associated with them.

SR 3.3.7.<sup>9</sup>

A CHANNEL CALIBRATION is performed every [18] months, or approximately at every refueling. CHANNEL CALIBRATION is a complete check of the instrument loop, including the sensor. The test verifies that the channel responds to a measured parameter within the necessary range and accuracy.

The Frequency is based on operating experience and is consistent with the typical industry refueling cycle.

---

REFERENCES

None. 1. WCAP-15376, Rev. 0, October 2000.

---

WOG STS

B 3.3-167

Rev 1, 04/07/95

**ACTIONS**

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

**SURVEILLANCE REQUIREMENTS**

SURVEILLANCE	FREQUENCY
SR 3.3.9.1 Perform COT.	[92] days 184
SR 3.3.9.2 Perform CHANNEL CALIBRATION.	[18] months

BDPS  
B 3.3.9**BASES****ACTIONS**B.1, B.2.1, B.2.2.1, and B.2.2.2 (continued)

once per 12 hours thereafter. This backup action is intended to confirm that no unintended boron dilution has occurred while the BDPS was inoperable, and that the required SDM has been maintained. The specified Completion Time takes into consideration sufficient time for the initial determination of SDM and other information available in the control room related to SDM.

**SURVEILLANCE REQUIREMENTS**

The BDPS trains are subject to a COT and a CHANNEL CALIBRATION.

SR 3.3.9.1

SR 3.3.9.1 requires the performance of a COT every [92] days, to ensure that each train of the BDPS and associated trip setpoints are fully operational. This test shall include verification that the boron dilution alarm setpoint is equal to or less than an increase of twice the count rate within a 10 minute period. The Frequency of [92] days is consistent with the requirements for source range channels in WCAP-2021-PA (Ref. 2).

184

15376

SR 3.3.9.2

SR 3.3.9.2 is the performance of a CHANNEL CALIBRATION every [18] months. CHANNEL CALIBRATION is a complete check of the instrument loop, including the sensor. The test verifies that the channel responds to a measured parameter within the necessary range and accuracy. For the BDPS, the CHANNEL CALIBRATION shall include verification that on a simulated or actual boron dilution flux doubling signal the centrifugal charging pump suction valves from the RMST open, and the normal CVCS volume control tank discharge valves close in the required closure time of  $\leq 20$  seconds.

The Frequency is based on operating experience and consistency with the typical industry refueling cycle.

(continued)

WOG STS

B 3.3-178

Rev 1, 04/07/95

**BASES (continued)**

---

**REFERENCES**

1. FSAR, Chapter [15].
  2. WCAP-1027X-PA / Supplement 2, Revision 1, June 1990.  
*15376, Rev 0, October 2000.*
-

## APPENDIX C

### FAULT TREE DIAGRAMS

The information provided in this Appendix is proprietary to Westinghouse Electric Company LLC. The coding associated with this information is " a,c"; therefore, it has not been included.